

# HP StorageWorks

## Enterprise File Services WAN Accelerator 3.0.4

### Management Console

#### user guide

## Legal and notice information

© Copyright 2006–2007 Hewlett-Packard Development Company, L.P.

© Copyright 2003–2007 Riverbed Technology, Inc.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided “as is” without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Linux is a trademark of Linus Torvalds in the United States and in other countries.

Microsoft, Windows, Windows NT, Windows 2000, Outlook, and Windows Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the United States and in other countries.

UNIX is a registered trademark in the United States and in other countries, exclusively licensed through X/Open Company, Ltd.

Parts of this product are derived from the following software:

Apache © 2000-2003 The Apache Software Foundation. All rights reserved.

bsdstr.c, © 1998 Todd C. Miller (Todd.Miller@courtesan.com). All rights reserved.

Busybox, © Eric Andersen

Less © 1984-2002 Mark Nudelman

Libevent, © 2000-2002 Niels Provos. All rights reserved.

LibGD, Version 2.0 licensed by Boutell.Com, Inc.

Libtecla, © 2000, 2001 by Martin C. Shepherd. All rights reserved.

Linux Kernel, © Linus Torvalds

md5, md5.cc, © 1995 University of Southern California. All rights reserved. © 1991-2, RSA Data Security, Inc. All rights reserved.

my\_getopt.{c,h}, © 1997, 2000, 2001, 2002, Benjamin Sittler. All rights reserved.

NET-SNMP: © 1989, 1991, 1992 by Carnegie Mellon University. All rights reserved.

OpenSSH, © 2002 Nils Nordman. All rights reserved.

ptmalloc © 2001 Wolfram Gloger

sSMTP, © Mark Ryan, Hugo Haas, Christoph Lameter, and Dave Collier-Brown

Vixie-Cron, © 1988,1990,1993,1994 by Paul Vixie. All rights reserved.

Zile, © 1997-2001 Sandro Sigalam © 2003 Reuben Thomas. All rights reserved.

For detailed copyright and license agreements, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. For modified source code (where required), see the HP technical support site at <http://www.hp.com>.

Certain libraries were used in the development of this software, licensed under GNU Lesser General Public License, Version 2.1, February 1999. For the copyright and license agreement, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*. For a list of libraries and source material (where required), see the HP technical support site at <http://www.hp.com>.

# Contents

<b>Introduction</b>	<b>7</b>
About This Guide	7
Types of Users	7
Organization of This Guide	7
Document Conventions	8
Hardware and Software Dependencies	8
Ethernet Network Compatibility	9
Antivirus Compatibility	9
Additional Resources	10
Related HP Documentation	10
Online Documentation	10
Related Reading	11
Contacting HP	11
Technical Support	11
HP Storage Web Site	11
 <b>Chapter 1 Overview of the HP EFS WAN Accelerator Management Console</b>	 <b>13</b>
Connecting to the Management Console	13
Connecting to the Management Console	13
The Home: Welcome Page	15
Navigating in the Management Console	16
Navigating in the Management Console	16
 <b>Chapter 2 Configuring the HP EFS WAN Accelerator</b>	 <b>21</b>
Setting Optimization Services	22
Enabling In-Path and Out-of-Path Support	22
Setting In-Path Rules	25
Modifying In-Path Descriptions	30
Configuring CIFS Protocol Support	31
Configuring MAPI Protocol Options	34

Configuring MS-SQL Protocol Options.....	36
Enabling the NFS-Application Streamlining.....	38
Modifying NFS Server Settings .....	39
Enabling HSTCP Protocol Options .....	42
Enabling Connection Pooling.....	44
Enabling Transparent Prepopulation .....	46
Setting Host Parameters.....	52
Setting the Primary Interface.....	52
Setting In-Path Interfaces .....	54
Setting Auxiliary Interfaces.....	58
Setting Main Static Routes .....	59
Setting Static In-Path Routes.....	60
Setting the DNS.....	61
Modifying the Host Name.....	63
Mapping Hosts to IP Addresses .....	63
Setting Proxies.....	64
Setting Advanced Network Parameters .....	65
Enabling Asymmetric Routing Auto-Detection .....	66
Enabling Connection Forwarding.....	68
Enabling Encryption.....	70
Enabling Failover and Data Store Synchronization .....	73
Enabling NetFlow.....	77
Setting Peering Rules .....	79
Enabling Quality of Service .....	81
Modifying a QoS Class .....	85
Setting QoS Marking.....	87
Modifying QoS Marking Descriptions.....	89
Modifying Service Ports.....	90
Enabling Simplified Routing.....	92
Enabling WCCP Groups .....	94
Modifying WCCP Group Settings .....	96
Enabling Proxy File Service .....	99
Enabling PFS .....	99
Adding PFS Shares.....	102
Creating Port Labels .....	113
Creating Port Labels.....	113
Modifying Ports in a Port Label .....	115
Setting Report Parameters.....	115
Setting Alarm Parameters.....	116
Setting Email Notification.....	117
Setting SNMP Parameters .....	119
Setting SNMP Trap Receivers.....	120
Setting Monitored Ports.....	121
Setting Logging Options .....	123
Setting Local Logging .....	123
Setting Remote Logging.....	124
Setting the Date and Time.....	125

Setting the Date and Time .....	125
Setting NTP Servers .....	126
Setting Authentication Methods .....	127
Setting General Authentication .....	127
Setting the Administrative Password .....	129
Setting the Monitor Password .....	130
Setting RADIUS Servers .....	131
Setting TACACS+ Servers .....	133
Modifying Web Settings .....	135
Setting the Message of the Day (MOTD) .....	136
Managing Licenses .....	137
Updating Your Licenses .....	137
Viewing Scheduled Jobs .....	138
Viewing Scheduled Jobs .....	139
Managing Configurations .....	139
Upgrading Your Software .....	142
Starting and Stopping Services .....	144
Rebooting the HP EFS WAN Accelerator .....	145
Shutting Down the HP EFS WAN Accelerator .....	145
 <b>Chapter 3   Creating HP EFS WAN Accelerator Reports and Logs .....</b>	 <b>147</b>
Creating Performance Reports .....	147
Creating Bandwidth Optimization Reports .....	148
Creating Data Store Hits Reports .....	150
Creating Data Reduction Reports .....	152
Creating NFS Statistics Report .....	155
Creating Throughput Reports .....	157
Creating Traffic Summary Reports .....	159
Viewing Appliance Reports .....	162
Viewing Data Store Reports .....	162
Viewing TCP Statistics Report .....	163
Viewing Networking Reports .....	165
Viewing Connected Appliances Reports .....	166
Viewing Connection History .....	167
Viewing Current Connections .....	170
Viewing the Current Connection Details Report .....	172
Viewing Connection Pooling .....	174
Viewing Interface Statistics .....	177
Creating Link State Reports .....	178
Creating Neighbor Statistic Reports .....	181
Creating QoS Statistics Reports .....	182
Viewing System Health Reports .....	185
Viewing Alarm Status Reports .....	185
Creating CPU Utilization Reports .....	188

Creating Memory Paging Reports.....	190
Viewing Proxy File Service Reports.....	192
Viewing PFS Share Status Reports.....	192
Viewing PFS Statistics .....	193
Exporting Performance Statistics Reports .....	196
Exporting Performance Statistics .....	196
Viewing System Diagnostic Files .....	197
Viewing System Dump Files .....	197
Viewing System Snapshots.....	198
Viewing TCP Dump Files .....	199
Viewing HP EFS WAN Accelerator Logs .....	200
Viewing HP EFS WAN Accelerator Logs.....	201
Getting Help.....	202
Contacting Technical Support .....	202
Viewing Online Help Contents.....	202
 <b>Appendix A HP EFS WAN Accelerator Ports .....</b>	<b>203</b>
Default Ports .....	203
Commonly Optimized Ports .....	204
Commonly Excluded Ports .....	204
Interactive Ports Forwarded by the HP EFS WAN Accelerator .....	205
Secure Ports Forwarded by the HP EFS WAN Accelerator .....	206
 <b>Appendix B HP EFS WAN Accelerator MIB .....</b>	<b>209</b>
Accessing the HP EFS WAN Accelerator Enterprise MIB .....	209
SNMP Traps.....	210
HP EFS WAN Accelerator Enterprise MIB.....	211
 <b>Glossary .....</b>	<b>225</b>
 <b>Index .....</b>	<b>229</b>

# Introduction

## In This Introduction

Welcome to the *HP EFS WAN Accelerator Management Console User Guide*. Read this introduction for an overview of the information provided in this guide and for an understanding of the documentation conventions used throughout. This introduction contains the following sections:

- ◆ [“About This Guide,”](#) next
- ◆ [“Hardware and Software Dependencies”](#) on page 8
- ◆ [“Ethernet Network Compatibility”](#) on page 9
- ◆ [“Antivirus Compatibility”](#) on page 9
- ◆ [“Additional Resources”](#) on page 10
- ◆ [“Contacting HP”](#) on page 11

---

## About This Guide

The *HP EFS WAN Accelerator Management Console User Guide* describes how to manage and monitor the HP StorageWorks Enterprise File Services WAN Accelerator using the Management Console.

## Types of Users

This guide is written for storage and network administrators with familiarity administering and managing networks using Common Internet File System (CIFS), Hypertext Transport Protocol (HTTP), File Transfer Protocol (FTP), and Microsoft Exchange.

## Organization of This Guide

The *HP EFS WAN Accelerator Management Console User Guide* includes the following chapters:

- ◆ [Chapter 1, “Overview of the HP EFS WAN Accelerator Management Console,”](#) describes how to connect to and navigate in the Management Console.
- ◆ [Chapter 2, “Configuring the HP EFS WAN Accelerator,”](#) describes how to configure and manage the HP EFS WAN Accelerator using the Management Console.

- ◆ [Chapter 3, “Creating HP EFS WAN Accelerator Reports and Logs,”](#) describes how to create and view HP EFS WAN Accelerator reports and logs.
- ◆ [Appendix A, “HP EFS WAN Accelerator Ports,”](#) provides a list of commonly optimized ports, excluded ports, default ports, and interactive and secure ports that are automatically forwarded by the HP EFS WAN Accelerator.
- ◆ [Appendix B, “HP EFS WAN Accelerator MIB,”](#) provides a reference for the HP EFS WAN Accelerator Enterprise Simple Network Management Protocol (SNMP) Message Information Block (MIB).

A glossary of terms follows the chapters, and a comprehensive index directs you to areas of particular interest.

## Document Conventions

This manual uses the following standard set of typographical conventions to introduce new terms, illustrate screen displays, describe command syntax, and so forth.

Convention	Meaning
<i>italics</i>	Within text, new terms and emphasized words appear in italic typeface.
<b>boldface</b>	Within text, commands, keywords, identifiers (names of classes, objects, constants, events, functions, program variables), environment variables, filenames, Graphical User Interface (GUI) controls, and other similar terms appear in bold typeface.
Courier	Information displayed on your terminal screen and information that you are instructed to enter appear in Courier font.
KEYSTROKE	Keys that you are to press appear in uppercase letters in Helvetica font.

## Hardware and Software Dependencies

The following table summarizes the hardware, software, and operating system requirements for the Management Console.

HP EFS WAN Accelerator Component	Hardware Requirements	Software Requirements Operating System Requirements
Management Console	<ul style="list-style-type: none"> <li>Any computer that supports a Web browser with a color image display.</li> </ul>	<ul style="list-style-type: none"> <li>The Management Console has been tested with Mozilla Firefox, version 1.0.x and 1.5.x and Microsoft Internet Explorer version 6.0x.</li> </ul> <p><b>NOTE:</b> Javascript and cookies must be enabled in your browser.</p> <p><b>NOTE:</b> If you want to encrypt your communication, you must have a Secure Sockets Layer (SSL) capable browser.</p>



## Ethernet Network Compatibility

The HP EFS WAN Accelerator supports the following types of Ethernet networks:

- ◆ Ethernet Logical Link Control (LLC) (IEEE 802.2 - 2002)
- ◆ Fast Ethernet 100 Base-TX (IEEE 802.3 - 2002)
- ◆ Gigabit Ethernet over Copper 1000 Base-T and Fiber 1000 Base-SX (LC connector) (IEEE 802.3 - 2002)

The Primary port in the HP EFS WAN Accelerator is 10 Base-T/100, Base-TX/1000, and Base-T/SX Mbps (IEEE 802.3 -2002).

In-path HP EFS WAN Accelerator ports are 10/100/1000 Base-TX or Gigabit Ethernet 1000Base-T/SX (IEEE 802.3 – 2002) (depending on your order).

The HP EFS WAN Accelerator supports Virtual Local Area Network (VLAN) Tagging (IEEE 802.1Q - 2003). It does not support the Cisco InterSwitch Link (ISL) protocol.

All copper interfaces are auto-sensing for speed and duplex (IEEE 802.3 - 2002).

The HP EFS WAN Accelerator auto-negotiates speed and duplex mode for all data rates and supports full duplex mode and flow control (IEEE 802.3 – 2002).

The HP EFS WAN Accelerator with a Gigabit Ethernet card supports Jumbo Frames on in-path and primary ports.

## Antivirus Compatibility

The HP EFS WAN Accelerator has been tested with the following antivirus software with no impact on performance:

- ◆ Network Associates (McAfee) VirusScan v7.0.0 Enterprise on the server
- ◆ Network Associates (McAfee) VirusScan v7.1.0 Enterprise on the server
- ◆ Network Associates (McAfee) VirusScan v7.1.0 Enterprise on the client
- ◆ Symantec (Norton) AntiVirus Corporate Edition v8.1 on the server

The HP EFS WAN Accelerator has been tested with the following antivirus software with a noticeable to moderate impact on performance:

- ◆ F-Secure Anti-Virus v5.43 on the client
- ◆ F-Secure Anti-Virus v5.5 on the server
- ◆ Network Associates (McAfee) NetShield v4.5 on the server
- ◆ Network Associates VirusScan v4.5 for multiplatforms on the client
- ◆ Symantec (Norton) AntiVirus Corporate Edition v8.1 on the client

---

## Additional Resources

This section describes the following resources that supplement the information in this guide:

- ◆ “Related HP Documentation” on page 10
- ◆ “Online Documentation” on page 10
- ◆ “Related Reading” on page 11

### Related HP Documentation

You can access the complete document set for the HP EFS WAN Accelerator from the *HP StorageWorks EFS WAN Accelerator Documentation Set CD-ROM*:

- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide* describes how to install and configure the HP EFS WAN Accelerator.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Command Line Interface Reference Manual* is a reference manual for the HP EFS WAN Accelerator command-line interface for the HP EFS WAN Accelerator. It lists commands, syntax, parameters, and example usage.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide* describes how to deploy the HP EFS WAN Accelerator in complex network environments (for example, environments using Web Cache Communication Protocol (WCCP), Policy-Based Routing (PBR), and Layer-4 switches).
- ◆ *HP StorageWorks Enterprise File Services Remote Copy Utility Reference Manual* describes how to install and deploy the HP EFS Remote Copy Utility (RCU). The RCU is an optional utility of the HP EFS WAN Accelerator that copies, mirrors, and transparently prepopulates data. You can download the RCU from the HP Technical Support site located at <http://www.hp.com>.
- ◆ *HP StorageWorks Enterprise File Services WAN Accelerator Manager User's Guide* describes how to install, configure, and administer a network made up of multiple HP EFS WAN Accelerators using the HP StorageWorks Enterprise File Services WAN Accelerator Manager.
- ◆ *HP StorageWorks Enterprise File Services N4c WAN Accelerator 4-port NIC Installation Guide* describes how to install bypass cards in the HP EFS WAN Accelerator.

### Online Documentation

The HP EFS WAN Accelerator documentation set is periodically updated with new information. To access the most current version of the HP EFS WAN Accelerator documentation and other technical information, consult the HP Technical Support site located at <http://www.hp.com>.

## Related Reading

To learn more about network storage systems and network administration, consult the following books:

- ◆ *Microsoft Windows 2000 Server Administrator's Companion* by Charlie Russell and Sharon Crawford (Microsoft Press, 2000)
- ◆ *Common Internet File System (CIFS) Technical Reference* by the Storage Networking Industry Association (Storage Networking Industry Association, 2002)
- ◆ *TCP/IP Illustrated, Volume I, The Protocols* by W. R. Stevens (Addison-Wesley, 1994)
- ◆ *Internet Routing Architectures (2nd Edition)* by Bassam Halabi (Cisco Press, 2000)

---

## Contacting HP

This section describes how to contact departments within HP.

## Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: <http://www.hp.com/support>. From this web site, select the country of origin. For example, the North American technical support number is 800-633-3600.

---

**NOTE:** For continuous quality improvement, calls may be recorded or monitored.

---

Be sure to have the following information available before calling:

- ◆ Technical support registration number (if applicable)
- ◆ Product serial numbers
- ◆ Product model names and numbers
- ◆ Applicable error messages
- ◆ Operating system type and revision level
- ◆ Detailed, specific questions

---

## HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access the storage site at: <http://www.hp.com/country/us/en/prodserv/storage.html>. From this web site, select the appropriate product or solution.



## CHAPTER 1

# Overview of the HP EFS WAN Accelerator Management Console

## In This Chapter

This chapter introduces the Management Console. This chapter includes the following sections:

- ◆ [“Connecting to the Management Console,”](#) next
- ◆ [“Navigating in the Management Console”](#) on page 16

---

**NOTE:** If you prefer, you can use the HP EFS WAN Accelerator Command Line Interface (CLI) to perform configuring and monitoring tasks. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command Line Interface Reference Manual*.

---

This chapter assumes you have installed and configured the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

This chapter also assumes you are familiar with the various deployment options available to you. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

---

## Connecting to the Management Console

You can connect to the Management Console through any supported Web browser.

## Connecting to the Management Console

To connect to the Management Console you must know the Uniform Resource Locator (URL) and administrator password that you assigned in the configuration wizard of the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

---

**NOTE:** Cookies and Javascript must be enabled in your Web browser.

---

## To connect to the Management Console

1. Enter the URL for the Management Console in the location box of your Web browser:

*protocol://host.domain*

*protocol* is **http** or **https**. Hypertext Transport Protocol Secure (HTTPS) uses the Secure Sockets Layer (SSL) protocol to ensure a secure environment. If you use HTTPS to connect, you are prompted to inspect and verify the SSL key.

*host* is the host name you assigned to the HP EFS WAN Accelerator during initial configuration. If your Domain Name Service (DNS) server maps that IP address to a name, you can specify the DNS name.

*domain* is the full domain name for the appliance.

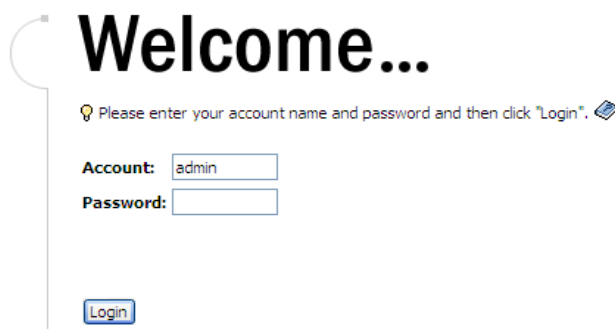
---

**TIP:** Alternatively, you can specify the IP address instead of the host and domain name.

---

The Management Console appears, displaying the Welcome page.

**Figure 1-1.** Welcome Page



Welcome...

Please enter your account name and password and then click "Login".

Account:

Password:

Login

2. In the **Account** text box, type the user login: **admin**, **monitor**, or a login from a Remote Authentication Dial-In User Service (RADIUS), or a Terminal Access Controller Access Control System (TACACS+) database. The default login is **admin**.

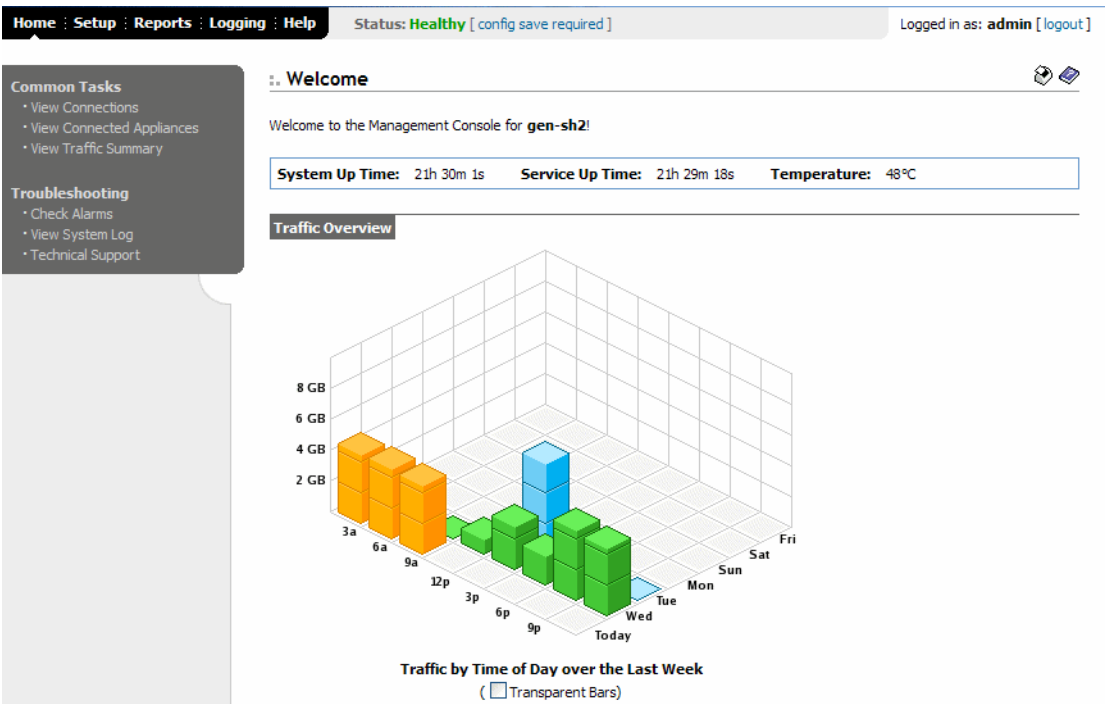
Users with administrator (**admin**) privileges can configure and administer the HP EFS WAN Accelerator. Users with monitor (**monitor**) privileges can view HP EFS WAN Accelerator reports and system logs.

3. In the **Password** text box, type the password you assigned in the configuration wizard of the HP EFS WAN Accelerator. (The HP EFS WAN Accelerator is shipped with the default password: **password**.)
4. Click **Login** to display the Home: Welcome page. The Home: Welcome page summarizes the current status of your system and provides links to connected appliances, a traffic summary, alarms, system logs, and technical support information.

# The Home: Welcome Page

The Management Console Home: Welcome page includes the current status of the HP EFS WAN Accelerator and the Traffic Overview report.

Figure 1-2. The Home: Welcome Page



The following table describes the information included in the Home: Welcome page.

Field	Description
Status Bar	<p>The status bar appears on every page of the Management Console and displays the current status of the system. To check the status of the system, click the link in the status bar. For detailed information about system alarms, see <a href="#">“Viewing Alarm Status Reports” on page 185</a>. The HP EFS WAN Accelerator can be in one of the following states:</p> <ul style="list-style-type: none"><li>• <b>Healthy.</b> All systems are functioning properly.</li><li>• <b>Degraded.</b> A system alarm has been triggered. Alarms are triggered for software version mismatches, abnormal memory page swapping activity, when the CPU utilization threshold has been reached, or on the Series 5000 and 3000, if there is a Redundant Array of Independent Disks (RAID) issue. For detailed information about system alarms, see <a href="#">“Viewing Alarm Status Reports” on page 185</a>.</li><li>• <b>Critical.</b> Critical indicates one of the following states:<ul style="list-style-type: none"><li>– <b>Bypass Mode.</b> The HP EFS WAN Accelerator service is not functioning or the HP EFS WAN Accelerator is in bypass mode. For detailed information, see <a href="#">“Starting and Stopping Services” on page 144</a>.</li><li>– <b>Unlicensed.</b> The HP EFS WAN Accelerator does not have a base license key or the key has expired. For detailed information, see <a href="#">“Updating Your Licenses” on page 137</a>.</li><li>– <b>Corrupted Store.</b> The HP EFS WAN Accelerator data store is corrupt. For detailed information, see <a href="#">“Starting and Stopping Services” on page 144</a>.</li><li>– <b>Service Halted.</b> The HP EFS WAN Accelerator has detected a software error that prevents the HP EFS WAN Accelerator service from continuing. For detailed information, see <a href="#">“Starting and Stopping Services” on page 144</a>.</li></ul></li><li>• <b>Connection Limit.</b> The system has reached the maximum number of connections for this model of the HP EFS WAN Accelerator. For detailed information about system alarms, see <a href="#">“Viewing Alarm Status Reports” on page 185</a>.</li></ul> <p><b>TIP:</b> The status bar alerts you if you need to save your configuration changes to memory. To save your changes, click the link in the status bar.</p>
System Up Time	Total time the system has been active.
Service Up Time	The state of the HP EFS WAN Accelerator service. The total time the HP EFS WAN Accelerator has been running or <b>Not Running</b> is displayed. To restart the HP EFS WAN Accelerator service, see <a href="#">“Starting and Stopping Services” on page 144</a> .
Temperature	The current Central Processing Unit (CPU) temperature. An alarm is raised if the temperature rises above 70° C.

## Navigating in the Management Console

The following section describes how to navigate in the Management Console.

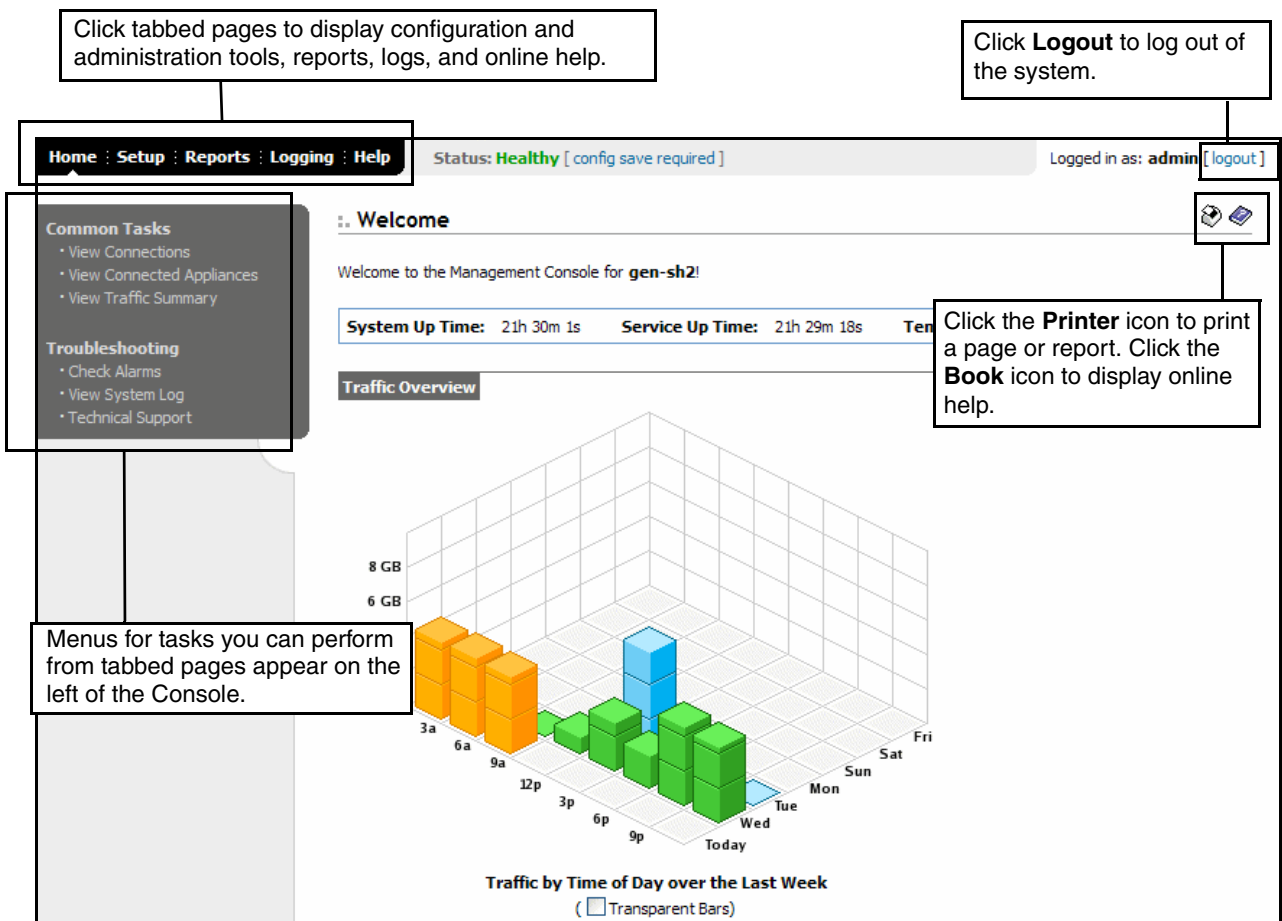
### Navigating in the Management Console

You navigate to the tools and reports available to you in the Management Console using hyperlinked tabs and menus.



The following figure illustrates the tabs and menus that appear on each page of the Management Console.

**Figure 1-3.** Management Console, The Home: Welcome Page



**TIP:** To revisit the Home: Welcome page, click **Home** in the navigation bar.

## Tabbed Pages and Menus

You click the hyperlinked tabs to display tools and reports to help you configure and manage your HP EFS WAN Accelerator. The following table summarizes the purpose of each tabbed page.

Tab	Purpose
Home	Displays the current status of your system and provides links to connected appliances, a traffic summary, alarms, system logs, and technical support information.
Setup	Configure and administer the HP EFS WAN Accelerator.
Reports	Create and view performance, network, and appliance reports.
Logging	View system logs.
Help	Display contact information for technical support, and the online-help table of contents.

When you click a hyperlinked tab, a menu for the tasks you can perform appears in the left menu of the Management Console. For example, when you click the Setup tab, the Setup menu appears.

Menu items are hyperlinks to pages that display tools and reports to help you configure and manage your HP EFS WAN Accelerator. When you click a menu item, you display the primary tool or report for the menu choice.

## Saving Your Configuration

As you **Apply** page settings, the values are applied to the running configuration and an orange exclamation point (!) appears in the left menu to remind you to permanently save your configuration settings to disk.

---

**NOTE:** The status bar at the top of each page also alerts you if the changes you have made require you to save them to disk. To save your changes, click the link in the status bar to go to the Configuration Manager page.

---

For detailed information about saving your configuration to disk, see [“Managing Configurations” on page 139](#).

## Restarting the HP EFS WAN Accelerator Service

Some configuration settings apply to the HP EFS WAN Accelerator service. The HP EFS WAN Accelerator service is a daemon that executes in the background performing operations when required.

If the new settings require you to restart the HP EFS WAN Accelerator service an orange exclamation point (!) appears in the left menu to remind you to restart the service. For detailed information, see [“Starting and Stopping Services” on page 144](#).

## Printing Pages and Reports

You can print Management Console pages and reports.

To print pages and reports



- Click the **Printer** icon in the upper right-side of the page to display a printer-friendly version of the page.

## Displaying Online Help



### To display online help

You can view online help that describes each page of the Management Console and the tasks that you can perform.

- Click the **Book** icon in the upper right-side of the page. The help for the page appears in a new browser window.

The Help tab provides you with the following links to help you administer and manage the HP EFS WAN Accelerator:

- ◆ **Technical Support.** Displays HP Technical Support contact information.
- ◆ **Online Help.** Displays the online help table of contents.

## Logging Out

Click the **Logout** link to end your session and require subsequent users to authenticate their session. When you click **Logout**, the Management Console displays the Good-Bye page.

### To log out of the Management Console

- Click **Logout** to display the Good-Bye page and log out of the Management Console.



## CHAPTER 2

# Configuring the HP EFS WAN Accelerator

## In This Chapter

This chapter describes how to configure and manage the HP EFS WAN Accelerator using the Management Console. This chapter includes the following sections:

- ◆ “Setting Optimization Services,” next
- ◆ “Setting Host Parameters” on page 52
- ◆ “Setting Advanced Network Parameters” on page 65
- ◆ “Enabling Proxy File Service” on page 99
- ◆ “Creating Port Labels” on page 113
- ◆ “Setting Report Parameters” on page 115
- ◆ “Setting Logging Options” on page 123
- ◆ “Setting the Date and Time” on page 125
- ◆ “Setting Authentication Methods” on page 127
- ◆ “Managing Licenses” on page 137
- ◆ “Viewing Scheduled Jobs” on page 138
- ◆ “Managing Configurations” on page 139
- ◆ “Upgrading Your Software” on page 142
- ◆ “Starting and Stopping Services” on page 144
- ◆ “Rebooting the HP EFS WAN Accelerator” on page 145
- ◆ “Shutting Down the HP EFS WAN Accelerator” on page 145

This chapter assumes that you have installed and configured the HP EFS WAN Accelerator. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide*.

If you prefer, you can use the HP EFS WAN Accelerator Command Line Interface (CLI) to configure your system. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command Line-Interface Reference Manual*.

---

## Setting Optimization Services

This section describes how to set optimization service parameters for the HP EFS WAN Accelerator. It includes the following sections:

- ◆ [“Enabling In-Path and Out-of-Path Support,”](#) next
- ◆ [“Setting In-Path Rules”](#) on page 25
- ◆ [“Modifying In-Path Descriptions”](#) on page 30
- ◆ [“Configuring CIFS Protocol Support”](#) on page 31
- ◆ [“Configuring MAPI Protocol Options”](#) on page 34
- ◆ [“Configuring MS-SQL Protocol Options”](#) on page 36
- ◆ [“Enabling the NFS-Application Streamlining”](#) on page 38
- ◆ [“Modifying NFS Server Settings”](#) on page 39
- ◆ [“Enabling HSTCP Protocol Options”](#) on page 42
- ◆ [“Enabling Connection Pooling”](#) on page 44
- ◆ [“Enabling Transparent Prepopulation”](#) on page 46
- ◆ [“Enabling and Synchronizing Prepopulation Shares”](#) on page 47

### Enabling In-Path and Out-of-Path Support

You can modify general in-path and out-of-path interface settings in the Optimization Service - General Settings Page.

---

**NOTE:** You were prompted to enable in-path or out-of-path support when you completed the installation wizard. This section describes how you can modify these settings.

---

The following types of deployments are available to you:

- ◆ **Physical In-Path.** The HP EFS WAN Accelerator is physically in the direct path between the client and server. The clients and servers continue to see client and server IP addresses. Physical in-path configurations are suitable for any location where the total bandwidth is within the limits of the installed HP EFS WAN Accelerator.
- ◆ **Virtual In-Path.** The HP EFS WAN Accelerator is virtually in the path between the client and server. This differs from a physical in-path in that a packet redirection mechanism is used to direct packets to HP EFS WAN Accelerators that are not in the physical path. Redirection mechanisms include Web Cache Communication Protocol (WCCP), Layer 4 (L4) switches, and Policy-Based Routing (PBR). In this configuration, clients and servers continue to see client and server IP addresses.
- ◆ **Out-of-Path.** The HP EFS WAN Accelerator is not in the direct path between the client and the server. Servers see the IP address of the server-side HP EFS WAN Accelerator rather than the client IP address, which might impact security policies. An out-of-path configuration is suitable for data center locations where physically in-path or virtually in-path configurations are not possible.

For detailed information about in-path and out-of-path deployments, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

If you have an HP EFS WAN Accelerator that contains multiple two-port or four-port bypass cards, the Management Console displays options to enable in-path support for these ports. The number of these interface options depends on the number of pairs of Local Area Network (LAN) and Wide Area Network (WAN) ports that you have enabled in your HP EFS WAN Accelerator.

### To enable in-path or out-of-path support

1. Click the Setup tab to display the Optimization Service - General Settings page.

Figure 2-1. Optimization Service - General Settings Page

The screenshot shows the HP EFS WAN Accelerator Management Console interface. At the top, there is a navigation bar with tabs: Home, Setup, Reports, Logging, and Help. The Setup tab is active. To the right of the tabs, the status is 'Healthy' with a note '[ config save required ]'. The user is logged in as 'adm'.

On the left side, there is a navigation menu with the following items:

- Optimization Service |
  - General Settings «
  - In-Path Rules
  - Protocol: CIFS
  - Protocol: MAPI
  - Protocol: MS-SQL
  - Protocol: NFS
  - Protocol: HSTCP
  - Connection Pooling
  - Prepopulation
- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs
- Configuration Manager (1)
- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

The main content area is titled 'Optimization Service - General Settings'. It contains the following sections:

- In-Path**: Configure your base optimization service settings.
  - ☒ Enable In-Path Support
    - ☐ Reset Existing Client Connections on Start Up
    - ☐ Enable L4/PBR/WCCP Support on Interface **wan0\_0**
    - ☒ Enable Optimizations on Interface **inpath0\_0**
    - ☒ Enable Optimizations on Interface **inpath0\_1**
- Out-of-Path (for server-side appliances only)**
  - ☐ Enable Out-of-Path Support
- Connection Limit**
  - Per Source IP Connection Limit:

At the bottom right of the main content area, there are two buttons: 'Apply' and 'Save'.

2. Use the controls to complete the configuration, as described in the following table.

Control	Description
In-Path	<p><b>Enable In-Path Support.</b> Specify this option to enable optimization on traffic that is in the direct path of the client, server, and HP EFS WAN Accelerator.</p> <hr/> <p><b>Reset Existing Client Connections on Startup.</b> Specify this option to enable <i>kickoff</i>. If you enable kickoff, connections that exist when the HP EFS WAN Accelerator service is started and restarted are disconnected. When the connections are retried they are optimized.</p> <p>Generally, connections are short lived and kickoff is not necessary. It is suitable for very challenging remote environments. For example, in an environment with 128 kbps and 1.5 seconds of latency, you might want to abort an HTTP download so that your traffic is optimized, whereas in a remote branch-office with a T1 and 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff.</p> <p><b>NOTE:</b> Do not enable kickoff for in-path HP EFS WAN Accelerators that use auto-discovery or if you do not have an HP EFS WAN Accelerator on the remote side of the network.</p> <hr/> <p><b>Enable L4/PBR/WCCP Support on Interface &lt;interface_name&gt;.</b> Specify this option to enable optional, virtual in-path support on the named interface. External traffic redirection is supported only on the first in-path interface. The following redirection methods are available:</p> <ul style="list-style-type: none"> <li>• <b>Layer-4 Switch.</b> You enable Layer-4 switch support when you have multiple HP EFS WAN Accelerators in your network, so that you can manage large bandwidth requirements.</li> <li>• <b>Policy-Based Routing (PBR).</b> PBR allows you to define policies to route packets instead of relying on routing protocols. You enable PBR to redirect traffic that you want optimized by an HP EFS WAN Accelerator that is not in the direct physical path between the client and server.</li> <li>• <b>Web Cache Communication Protocol (WCCP).</b> If your network design requires you to use WCCP, a packet redirection mechanism directs packets to HP EFS WAN Accelerators that are not in the direct physical path to ensure that they are optimized.</li> </ul> <p>For detailed information about configuring Layer-4 switch, PBR, and WCCP deployments, see the <i>HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide</i>.</p> <hr/> <p><b>Enable Optimizations on Interface &lt;interface_name&gt;.</b> Specify this option to enable in-path support for additional bypass cards.</p> <p>If you have an HP EFS WAN Accelerator that contains multiple two-port or four-port bypass cards, the Management Console displays options to enable in-path support for these ports. The number of these interface options depends on the number of pairs of LAN and WAN ports that you have enabled in your HP EFS WAN Accelerator.</p> <p>The interface names for the bypass cards are a combination of the slot number and the port pairs (<b>inpath&lt;slot&gt;_&lt;pair&gt;</b>, <b>inpath&lt;slot&gt;_&lt;pair&gt;</b>). For example, if a four-port bypass card is located in <b>slot 0</b> of your appliance, the interface names are: <b>inpath0_0</b> and <b>inpath0_1</b>. Alternatively, if the bypass card is located in slot 1 of your appliance, the interface names are: <b>inpath1_0</b> and <b>inpath1_1</b>. The maximum number of pairs is six, which is three four-port bypass cards.</p> <p>For detailed information about installing additional bypass cards, see the <i>HP StorageWorks Enterprise File Services N4c WAN Accelerator 4-port NIC Installation Guide</i>.</p>



Control	Description
Out-of-Path	<p><b>Enable Out-of-Path Support.</b> Specify this option to enable out-of-path support. You enable out-of-path support on server-side HP EFS WAN Accelerators only.</p> <p><b>NOTE:</b> If you set up an out-of-path configuration with failover support, you must set fixed target rules that specify the master and backup HP EFS WAN Accelerators. For detailed information, see <a href="#">“Setting In-Path Rules” on page 25</a>.</p>
Connection Limit	<p><b>Per Source IP Connection Limit.</b> Check this box to limit half-opened connections on a source IP address initiating connections (that is, the client machine). Set this feature to block a source IP address that is opening multiple connections to invalid hosts or ports simultaneously (for example, a virus or a port scanner). This feature does not prevent a source IP address from connecting to valid hosts at a normal rate. Thus a source IP address could have more established connections than the limit. The default value is <b>4096</b>.</p> <p>The appliance counts the number of half-opened connections for a source IP address (connections that check if a server connection can be established before accepting the client connection). If the count is above the limit, new connections from the source IP address are passed through unoptimized.</p> <p><b>NOTE:</b> If you have a client connecting to valid hosts or ports at a very high rate, some of its connections might be passed through even though all the connections are valid.</p>

3. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting In-Path Rules

You set in-path configuration rules in the Optimization Service - In-Path Rules page.

An in-path rule defines the policies for intercepting traffic on specified ports for optimization.

You can create rules that apply to a single port or to a *port label*. A port label is a name that you assign to a set of ports so that you can reduce the number of configuration rules in your system. The following port labels are created by default in your system:

- ◆ **Interactive.** Automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell).
- ◆ **Secure.** Automatically pass-through traffic on commonly secure ports (for example, **ssh**, **https**, and **smtps**).
- ◆ **RBT-Proto.** Specifies well-known ports used by the system: **7800-7801** (in-path), **7810** (out-of-path), **7820** (failover), **7850** (connection forwarding), **7860** (Interceptor appliance).

If you do not want to automatically forward these ports, click **Remove Selected Rules** in the Optimization Service - In-Path Rules page.

For detailed information about how to configure port labels, see [“Creating Port Labels” on page 113](#).

For a list of interactive and secure ports that are automatically forwarded, see [Appendix A, “HP EFS WAN Accelerator Ports.”](#)

- To set an in-path rule
1. Click the Setup tab to expand the Optimization Service menu.

2. Click In-Path Rules to display the Optimization Service - In-Path Rules page.

Figure 2-2. Optimization Service - In-Path Rules Page

Home : Setup : Reports : Logging : Help

Status: Healthy

Logged in as: admin [logout]

Optimization Service

General Settings

In-Path Rules

Protocol: CIFS

Protocol: MAPI

Protocol: MS-SQL

Protocol: NFS

Connection Pooling

Prepopulation

Host Settings

Advanced Networking

Proxy File Service

Port Labels

Reports

Logging

Date & Time

Authentication

Licenses

Scheduled Jobs

Configuration Manager

Upgrade Software

Start/Stop Services

Reboot Appliance

Shutdown Appliance

Optimization Service - In-Path Rules

Configure your in-path rules. By default, all traffic going through this appliance is optimized. Note that only the first matching rule will be applied.

#	Type	Source	Destination	Port	Target	Port	Opt Policy	Neural	VLAN	
<input type="checkbox"/> 1	Pass	All	All	Secure	--	--	--	--	All	<a href="#">[edit desc]</a>
<input type="checkbox"/> 2	Pass	All	All	Interactive	--	--	--	--	All	<a href="#">[edit desc]</a>
<input type="checkbox"/> 3	Pass	All	All	RBT-Proto	--	--	--	--	All	<a href="#">[edit desc]</a>
def	Auto	All	All	All	--	--	Normal	Always	All	

Remove Selected Rules

Move Rule: 

1

 to 

start

Move Rule

Add New Rule:

Type: 

Auto Discover

 Insert Rule At: 

end

Source Subnet: 

0.0.0.0/0

 Destination Subnet: 

0.0.0.0/0

 Port: 

all

Advanced Options (click to open):

VLAN Tag ID: 

All

Optimization Policy: 

Normal

Neural Framing Mode: 

Always

Description:

Add Rule

Additional Options:

☐ Enable Computation of Neural Heuristics

Update Settings

26

CONFIGURING THE HP EFS WAN ACCELERATOR

## 3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Rule	<p><b>Type.</b> Select one of the following rule types from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Auto-Discovery.</b> Auto-discovery is the process by which the HP EFS WAN Accelerator automatically intercepts and optimizes traffic on all Internet Protocol (IP) addresses and ports. By default, auto-discovery is applied to all IP addresses and the ports which are not secure or interactive. Defining in-path rules modifies this default setting.</li> <li>• <b>Fixed-Target.</b> Use fixed-target rules to specify out-of-path HP EFS WAN Accelerators near the target server that you want to optimize. Determine which servers you would like a particular HP EFS WAN Accelerator to optimize (and, optionally, which ports), and add rules to specify the network of servers, ports, port labels, and out-of-path HP EFS WAN Accelerators to use.</li> <li>• <b>Pass-Through.</b> Pass-through rules identify traffic that is passed through the network unoptimized. You define pass-through rules to exclude subnets from optimization. Traffic is also passed through when the HP EFS WAN Accelerator is in bypass mode. (Pass through might occur because of in-path rules or because the connection was established before the HP EFS WAN Accelerator was put in place or before the HP EFS WAN Accelerator service was enabled.)</li> <li>• <b>Discard.</b> Packets for the connection that match the rule are dropped silently. The HP EFS WAN Accelerator filters out traffic that matches the discard rules. This process is similar to how routers and firewalls drop disallowed packets: the connection-initiating device has no knowledge of the fact that its packets were dropped until the connection times out.</li> <li>• <b>Deny.</b> When packets for connections match the deny rule, the appliance actively tries to reset the connection. Deny tells the HP EFS WAN Accelerator to actively try to reset a TCP connection being attempted. Using an active reset process, rather than a silent discard allows the connection initiator to know that its connection is disallowed.</li> </ul> <p>If you have an out-of-path configuration with failover support, you specify the master and backup HP EFS WAN Accelerator in the Optimization Service - In-Path Rules page.</p> <p><b>NOTE:</b> In out-of-path deployments, to optimize MAPI Exchange 2003 by destination port, you must define fixed-target, in-path rules that specify the following ports on the client-side HP EFS WAN Accelerator: the Microsoft end-point mapper port: <b>135</b>; the HP EFS WAN Accelerator port for Exchange traffic: <b>7830</b>; the HP EFS WAN Accelerator port for Exchange Directory Name Service Provider Interface (NSPI) traffic: <b>7840</b>. For detailed information, see <a href="#">“Optimizing MAPI Exchange in Out-of-Path Deployments” on page 34</a>.</p> <hr/> <p><b>Source Subnet.</b> Specify the IP address for the source network in the <b>Source Subnet</b> text box. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <hr/> <p><b>Destination Subnet.</b> Specify the IP address for the destination network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <hr/> <p><b>Port.</b> Specify the destination port number, port label, or <b>all</b>. For detailed information on port labels, see <a href="#">“Creating Port Labels” on page 113</a>.</p>

Control	Description
Add New Rule cont.	<p><b>Insert Rule At.</b> Select <b>start</b>, <b>end</b>, or a rule number from the drop-down list.</p> <p>HP EFS WAN Accelerators evaluate rules in numerical order starting with rule <b>1</b>. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule <b>1</b> do not match, rule <b>2</b> is consulted. If rule <b>2</b> matches the conditions, it is applied, and no further rules are consulted.</p> <p>In general, you should list rules in the following order:</p> <p><b>1. Pass-through.</b> List the exceptions to optimization, first.</p> <p><b>2. Fixed-target.</b> List any fixed-targets for optimization, next.</p> <p><b>3. Auto-discovery.</b> Apply the default rule: optimize all remaining traffic. (The default auto-discovery rule is listed automatically.)</p> <hr/> <p><b>Add Rule.</b> Specify this option to add the rule to the rules list.</p> <hr/> <p><b>Remove Selected Rules.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Rules</b>.</p> <hr/> <p><b>Move Rule.</b> Use the <b>Move Rule</b> drop-down list and button to change the order in which rules are evaluated.</p>

Control	Description
Advanced Options	<p><b>VLAN Tag ID.</b> Select the VLAN identification number from the drop-down list to set the VLAN tag identification number (VLAN ID). <b>All</b> specifies the rule applies to all VLANs; <b>Untagged</b> specifies the rule applies to non-tagged connections.</p> <p>The HP EFS WAN Accelerator supports VLAN 802.1q. To configure VLAN tagging you perform the following tasks:</p> <ul style="list-style-type: none"> <li>• You configure in-path rules to apply to all VLANs or to a specific VLAN. By default, rules apply to all VLAN values unless you specify a particular VLAN ID. Pass-through traffic maintains any pre-existing VLAN tagging between the LAN and WAN interfaces.</li> <li>• You set the in-path interfaces, VLAN tag IDs to define the VLAN tag that the HP EFS WAN Accelerator uses to communicate with other HP EFS WAN Accelerator. For detailed information, see <a href="#">“Setting In-Path Interfaces” on page 54</a>.</li> </ul> <hr/> <p><b>Optimization Policy.</b> Optionally, if you have selected an <b>Auto-Discovery</b> or <b>Fixed Target</b> rule, you can configure the following types of optimization policies:</p> <ul style="list-style-type: none"> <li>• <b>Normal.</b> Perform Lempel-Ziv (LZ) compression and Scalable Data Referencing (SDR).</li> <li>• <b>SDR-Only.</b> Perform SDR; do not perform LZ compression.</li> <li>• <b>Compression-Only.</b> Perform LZ compression; do not perform SDR.</li> <li>• <b>None.</b> Do not perform SDR or LZ compression.</li> </ul> <p>Setting an optimization policy allows you more flexibility in applying optimization techniques. For example, if you have a network that requires 45 Mbps or higher with abundant bandwidth, you do not need to perform LZ compression to obtain maximum optimization of data. Turning off LZ compression also increases throughput on large bandwidth networks.</p> <p>To configure optimization policies for the File Transfer Protocol (FTP) data channel, define an in-path rule with the destination port <b>20</b> and set its optimization policy. Setting QoS for port <b>20</b> on the client-side HP EFS WAN Accelerator effects passive FTP, while setting the QoS for port <b>20</b> on the server-side HP EFS WAN Accelerator effects active FTP.</p> <p>To configure optimization policies for the Messaging Application Protocol Interface (MAPI) data channel, define an in-path rule with the destination port <b>7830</b> and set its optimization policy.</p>

Control	Description
Advanced Options cont.	<p><b>Neural Framing.</b> Optionally, if you have selected <b>Auto-Discovery</b> or <b>Fixed Target</b>, you can select a neural framing mode for the in-path rule. Neural framing enables the appliance to select the optimal packet framing boundaries for SDR. Neural framing creates a set of heuristics to intelligently determine the optimal moment to flush TCP buffers. The appliance continuously evaluates these heuristics and uses the optimal heuristic to maximize the amount of buffered data transmitted in each flush, while minimizing the amount of idle time that the data sits in the buffer. You can specify the following neural framing settings:</p> <ul style="list-style-type: none"> <li>• <b>Never.</b> Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used.</li> <li>• <b>Always.</b> Always use the Nagle algorithm. All data is passed to the codec which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs up the codec and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used.</li> <li>• <b>Transmission Control Protocol (TCP) Hints.</b> This is the default setting which is based on the TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used.</li> <li>• <b>Dynamic.</b> Dynamically adjust the Nagle parameters. In this option, the HP EFS WAN Accelerator software discerns the optimum algorithm for a particular type of traffic and switches to the best algorithm based on traffic characteristic changes.</li> </ul> <p>For different types of traffic, one algorithm may be better than others. The considerations include: latency added to the connection, compression, and SDR performance.</p> <p>To configure neural framing for an FTP data channel, define an in-path rule with the destination port <b>20</b> and set its optimization policy. To configure neural framing for a MAPI data channel, define an in-path rule with the destination port <b>7830</b> and set its optimization policy.</p>
Additional Options	<p><b>Enable Computation of Neural Heuristics.</b> Optionally, check this box to enable optimal packet framing boundaries for SDR.</p> <hr/> <p><b>Update.</b> Click <b>Update</b> to apply your settings to the running configuration.</p> <hr/> <p><b>Remove Selected Rules.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Rules</b>.</p>

4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying In-Path Descriptions

You can modify the description of your in-path rules in the Optimization Service - In-Path Rules Edit page.

## To modify your in-path rule description

1. Click the Setup tab to expand the Optimization Service menu.
2. Click In-Path Rules to display the Optimization Service - In-Path Rules page.
3. Click **Edit Desc** in the Rules table to display the Optimization Service - In-Path Rules Edit page.

**Figure 2-3. Optimization Service - In-Path Rules Edit Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [config save required]    Logged in as: admin [logout]

Optimization Service |

- General Settings
- **In-Path Rules** «
- Protocol: CIFS
- Protocol: MAPI
- Protocol: MS-SQL
- Protocol: NFS
- Connection Pooling
- Prepopulation
- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs
- Configuration Manager (1)
- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

Optimization Service - In-Path Rules

Check and modify your in-path rule.

Description

test

Update Description    Cancel

Save    Reset

4. Modify the description of the rule in the text box and click **Update Description**.
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Configuring CIFS Protocol Support

You configure CIFS protocol support in the Optimization Service - Protocol: CIFS page.

CIFS optimization is enabled by default. Typically, you only disable CIFS optimization to troubleshoot the system.

## To configure CIFS protocol options

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Protocol: CIFS to display the Optimization Service - Protocol: CIFS page.

Figure 2-4. Optimization Service - Protocol: CIFS Page

The screenshot displays the 'Optimization Service - Protocol: CIFS' configuration page. The top navigation bar includes 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy', and the user is logged in as 'admin'. The left sidebar lists various configuration options under 'Optimization Service', with 'Protocol: CIFS' selected. The main content area is titled 'Optimization Service - Protocol: CIFS' and contains a lightbulb icon with the text 'Configure your CIFS protocol settings.' Below this, there are two sections: 'General' and 'Overlapping Open'. The 'General' section has four checkboxes: 'Enable Latency Optimization' (checked), 'Disable Write Optimization' (unchecked), 'Optimize Connections with Security Signatures (that do not require signing)' (checked), and 'Enable Dynamic Write Throttling' (checked). The 'Overlapping Open' section has a checked checkbox for 'Enable Overlapping Open Optimization.' and two radio button options for file extensions. The first option, 'Optimize Only the Following Extensions:', is selected, and the text box contains 'doc, pdf, ppt, sldasm, slddrw, slddwg, sldprt, txt, vsd, xls'. The second option, 'Optimize All Except the Following Extensions:', is unselected, and its text box contains 'ldb, mdb'. At the bottom right, there are 'Apply', 'Save', and 'Reset' buttons.

Home : Setup : Reports : Logging : Help Status: **Healthy** Logged in as: **admin** [logout]

**Optimization Service** |

- General Settings
- In-Path Rules
- **Protocol: CIFS** «
- Protocol: MAPI
- Protocol: MS-SQL
- Protocol: NFS
- Protocol: HSTCP
- Connection Pooling
- Prepopulation
- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

• Configuration Manager

• Upgrade Software

• Start/Stop Services

• Reboot Appliance

• Shutdown Appliance

**Optimization Service - Protocol: CIFS**

Configure your CIFS protocol settings.

**General**

- ☒ Enable Latency Optimization
- ☐ Disable Write Optimization
- ☒ Optimize Connections with Security Signatures (that do not **require** signing)
- ☒ Enable Dynamic Write Throttling

**Overlapping Open**

- ☒ Enable Overlapping Open Optimization.
- ☒ Optimize Only the Following Extensions:
- ☐ Optimize All Except the Following Extensions:

Apply Save Reset



## 3. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p><b>Enable Latency Optimization.</b> Latency optimization is enabled by default. Only uncheck this box if you want disable Latency optimization. Typically, you disable latency optimization to troubleshoot problems with the system.</p> <hr/> <p><b>Disable Write Optimization.</b> Specify this option to disable write optimization.</p> <p>Disable write optimization only if you have applications that assume and require write-through in the network. If you disable write optimization, the HP EFS WAN Accelerator still provides optimization for CIFS reads and for other protocols, but you might experience a slight decrease in overall optimization.</p> <p>Most applications operate safely with write optimization because CIFS allows you to explicitly specify write-through on each write operation. However, if you have an application that does not support explicit write-through operations, you must disable it in the HP EFS WAN Accelerator.</p> <p>If you do not disable write-through, the HP EFS WAN Accelerator acknowledges writes before they are fully committed to disk, to speed up write operation. The HP EFS WAN Accelerator does not acknowledge the file close until the file is safely written.</p> <hr/> <p><b>Optimize Connections with Security Signatures (that do not require signing).</b> Specify this option to disable Windows Server Message Block (SMB) signing.</p> <p>The Secure-CIFS feature enables you to automatically disable Windows Server Message Block (SMB) signing. SMB signing prevents the appliance from applying full optimization on CIFS connections and significantly reduces the performance gain from an HP EFS WAN Accelerator deployment. Because many enterprises already take additional security precautions (such as firewalls, internal-only reachable servers, and so forth), SMB signing adds little additional security, at a significant performance cost (even without appliances).</p> <p>Before you enable Secure-CIFS, you must consider the following factors:</p> <ul style="list-style-type: none"> <li>• If the client-side machine has <b>Required</b> signing, enabling Secure-CIFS prevents the client from connecting to the server.</li> <li>• If the server-side machine has <b>Required</b> signing, the client and server connect but you cannot perform full latency optimization with the appliance. Domain controllers default to <b>Required</b>.</li> </ul> <p>For detailed information about SMB signing and the performance cost associated with it, see the <i>HP StorageWorks Enterprise File Services WAN Accelerator Installation and Configuration Guide</i>.</p> <hr/> <p><b>Enable Dynamic Write Throttling.</b> Enables CIFS dynamic throttling mechanism which replaces the current static buffer scheme. If you enable CIFS dynamic throttling, it is activated only when there are sub-optimal conditions on the server side causing a backlog of writes messages; it does not have a negative effect under normal network conditions.</p>

Control	Description
Overlapping Open	<p><b>Enable Overlapping Open Optimization.</b> This option is enabled by default. To prevent any compromise to data integrity, the HP EFS WAN Accelerator only optimizes data to which exclusive access is available (in other words, when locks are granted). When an oplock is not available the HP EFS WAN Accelerator does not perform application-level latency optimizations but still performs Scalable Data Referencing (SDR) and compression on the data as well as TCP optimizations. If you disable this feature, the HP EFS WAN Accelerator will still increase WAN performance, but not as effectively.</p> <p>Enabling this feature on applications that perform multiple opens of the same file to complete an operation will result in a performance improvement (for example, Computer Aided Design (CAD) applications):</p> <ul style="list-style-type: none"> <li>• <b>Optimize the Following Extensions.</b> Specify a list of extensions you want to optimize using overlapping opens. The default values are: <b>doc, pdf, ppt, sldasm, slddrw, slddwg, sldprt, txt, vsd, xls.</b></li> <li>• <b>Do Not Optimize the Following Extensions.</b> Specify a list of extension you do not want to optimize using overlapping opens. The default values are: <b>ldb, mdb.</b></li> </ul> <p><b>NOTE:</b> If a remote user opens a file which is optimized using the overlapping opens feature and a second user opens the same file they might receive an error if the file fails to go through a v3.x HP EFS WAN Accelerator or if it does not go through an HP EFS WAN Accelerator (for example, certain applications that are sent over the LAN). If this occurs, you should disable overlapping opens for those applications.</p>

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Configuring MAPI Protocol Options

You configure MAPI protocol support in the Optimization Service - Protocol: MAPI Page.

MAPI optimization is enabled by default. Typically, you only disable MAPI optimization to troubleshoot the system.

## Optimizing MAPI Exchange in Out-of-Path Deployments

In out-of-path deployments, if you want to optimize MAPI Exchange by destination port, you must define a fixed-target, in-path rule that specifies the following ports on the client-side appliance:

- ◆ **Port 135.** The Microsoft end-point mapper port
- ◆ **Port 7830.** The HP EFS WAN Accelerator port used for Exchange traffic
- ◆ **Port 7840.** The HP EFS WAN Accelerator port used for Exchange Directory NSPI traffic

For detailed information about defining in-path rules, see [“To set an in-path rule” on page 26.](#)

### To configure MAPI protocol options

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Protocol: MAPI to display the Optimization Service - Protocol: MAPI page.

Figure 2-5. Optimization Service - Protocol: MAPI Page

Home
Setup
Reports
Logging
Help

Status: Healthy [ config save required ]

Logged in as: admin [ logout ]

Optimization Service
General Settings
In-Path Rules
Protocol: CIFS
Protocol: MAPI
Protocol: MS-SQL
Protocol: NFS
Connection Pooling
Prepopulation
Host Settings
Advanced Networking
Port Labels
Reports
Logging
Date & Time
Authentication
Licenses
Scheduled Jobs

Configuration Manager
Upgrade Software
Start/Stop Services
Reboot Appliance
Shutdown Appliance

### Optimization Service - Protocol: MAPI

Configure your MAPI protocol settings.

General

☒ Enable MAPI Optimization
☒ Enable MAPI NSPI. NSPI Port: 
☒ Enable MAPI Exchange 2003 Acceleration. Exchange 2003 Port:

MAPI Transparent Prepopulation

☒ Enable Transparent Prepopulation

Max Connections: 
Poll Interval:  minutes
Time Out:  hours

Apply

Save

Reset

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p><b>Enable MAPI Optimization.</b> MAPI optimization is enabled by default. Only uncheck this box if you want disable MAPI optimization. Typically, you disable MAPI optimization to troubleshoot problems with the system. For example, if you are experiencing problems with Outlook clients connecting with Exchange, you can disable MAPI latency acceleration (while continuing to optimize with SDR for MAPI).</p> <p><b>Enable MAPI NSPI Optimization.</b> NSPI optimization is enabled by default. Only uncheck this box if you want disable MAPI NSPI optimization. Typically, you disable MAPI NSPI optimization to troubleshoot problems with the system. NSPI is the address book subcomponent of the Exchange protocol that is optimized by the appliance. In certain situations (for example, clients connecting through a firewall), you might want to force a server to listen on a single pre-defined port so that access to ports can be controlled or locked down on the firewall.</p> <p><b>NSPI port.</b> Specify the NSPI port.</p> <p><b>Enable MAPI Exchange 2003 Acceleration.</b> Specify this option to enable MAPI 2003 Acceleration. This feature increases optimization of traffic between Exchange 2003 and Outlook 2003.</p>

Control	Description
	<p><b>MAPI Exchange 2003 Port.</b> Specify the MAPI Exchange 2003 port. Typically, you do not need to modify the default value, <b>7830</b>. If you have changed the Microsoft Exchange Information Store Interface (MEISI) port in your Exchange Server environment, change port <b>7830</b> to the static port number you have configured in your Exchange environment.</p> <p>For further information about changing (MEISI) ports, see the Microsoft Exchange Information Store Interface at <a href="http://support.microsoft.com/default.aspx?scid=kb;en-us;270836">http://support.microsoft.com/default.aspx?scid=kb;en-us;270836</a>.</p> <p><b>NOTE:</b> For out-of-path deployments, to optimize MAPI Exchange 2003, you must define fixed-target, in-path rules that specify the following ports on the client-side HP EFS WAN Accelerator: the Microsoft end-point mapper port: <b>135</b>; the HP EFS WAN Accelerator port for Exchange traffic: <b>7830</b>; the HP EFS WAN Accelerator port for Exchange Directory NSPI traffic: <b>7840</b>. For information on creating a fixed-target, in-path rule, see “<a href="#">Setting In-Path Rules</a>” on page 25.</p>
MAPI Transparent Pre-population	<p><b>Enable MAPI Transparent Pre-population.</b> Specify this option to enable MAPI transparent pre-population.</p> <p>This feature allows email data to be delivered between the Exchange server and the client-side appliance while the Outlook client is off-line. When a user logs into their MAPI client, the mail is already waiting in the client-side appliance and can be retrieved locally. This feature enables email to be optimized even though it has not been seen before by the client.</p> <hr/> <p><b>Max Connections.</b> Specify the maximum number of virtual MAPI connections to the Exchange server for Outlook clients that have shut down. Setting the maximum connections limits the aggregate load on all Exchange servers through the configured HP EFS WAN Accelerator. The default value is <b>325</b>.</p> <p>You must configure the maximum connections on both the client and server-side of the network.</p> <hr/> <p><b>Poll Interval.</b> Set the number of minutes you want the appliance to poll for shut down clients. The default is <b>20</b>.</p> <hr/> <p><b>Time-out.</b> Specify the number of hours after which to time-out virtual MAPI connections. When this threshold is reached, the virtual MAPI connection is terminated. The time-out is enforced on a per-connection basis. Time-out prevents a build up of stale or unused virtual connections over time. The default value is <b>96</b>.</p>

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Configuring MS-SQL Protocol Options

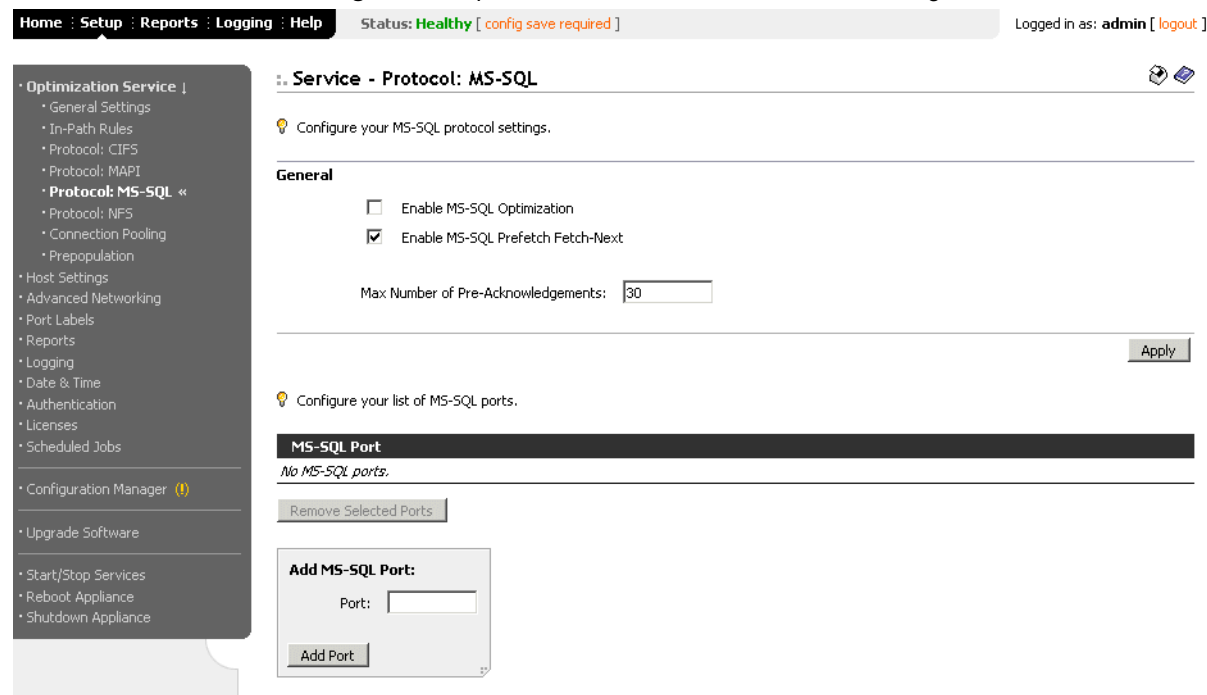
You configure MS-SQL protocol support in the Optimization Service - Protocol: MS-SQL page. Enabling MS-SQL optimization applies default rules to increase optimization for Microsoft Project (MS Project).

The MS-SQL feature also optimizes other database applications, but you must define SQL rules to obtain maximum optimization. If you are interested in enabling the MS-SQL feature for other database applications, contact HP professional services.

To configure MS-SQL protocol support

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Protocol: MS-SQL to display the Optimization Service - Protocol: MS-SQL page.

Figure 2-6. Optimization Service - Protocol: MS-SQL Page



3. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p><b>Enable MS-SQL Optimization.</b> Specify this option to increase optimization for Microsoft Project.</p> <p><b>Enable MS-SQL Prefetch Fetch-Next.</b> Specify this option to enable prefetching requests to request the next row in MS Project. This feature is enabled by default. The server-side appliance prefetches sequential row results and the client-side HP EFS WAN Accelerator caches them.</p> <p><b>Max Number of Pre-Acknowledgements.</b> Specify the number of requests to pre-acknowledge before waiting for a server response to be returned. The default is <b>30</b>.</p> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)</p>
Add MS-SQL Port	<p><b>Port.</b> Specify the port number for the MS-SQL server.</p> <p><b>Add Port.</b> Click <b>Add Port</b>. The default is <b>1433</b>.</p> <p><b>Remove Selected Ports.</b> To remove an entry, click the check box next to the port name and click <b>Remove Selected Ports</b>.</p>

# Enabling the NFS-Application Streamlining

You enable NFS-application streamlining in the Optimization Service - Protocol: NFS page. NFS-application streamlining provides latency optimization improvements for NFS operations primarily by prefetching data, storing it on the client HP EFS WAN Accelerator for a short amount of time, and using it to respond to client requests.

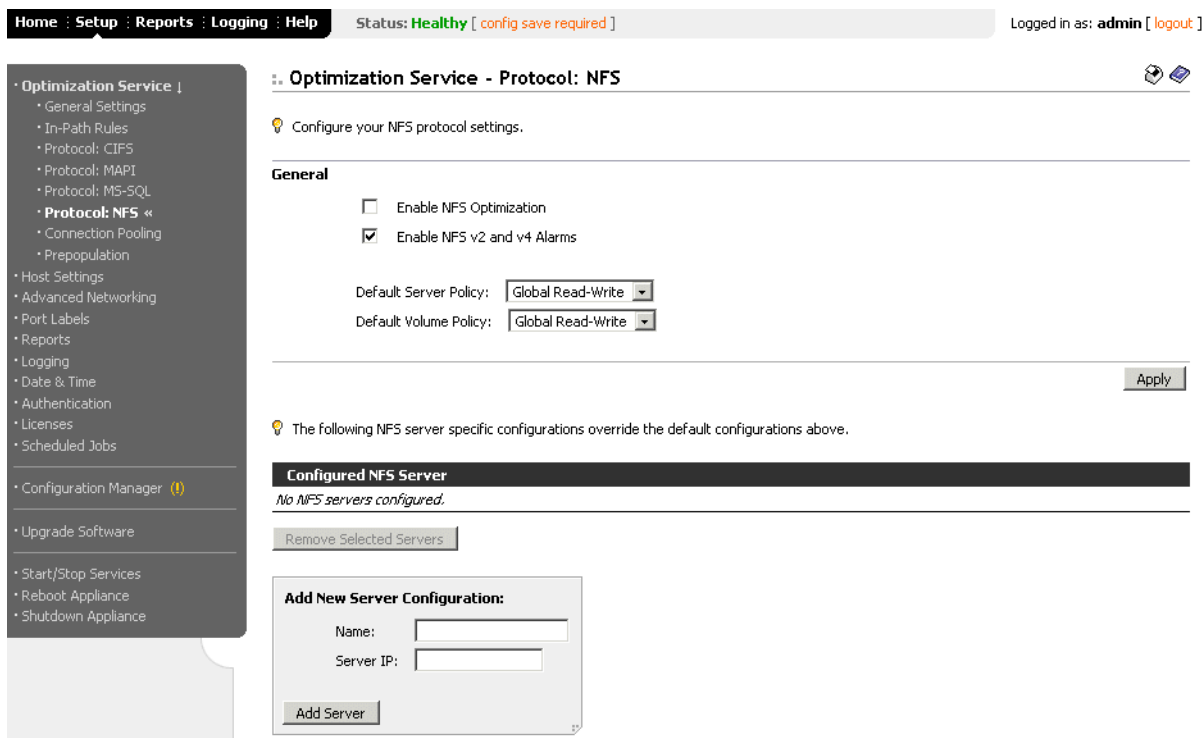
You enable NFS-application streamlining where NFS performance over the WAN is impacted by a high latency environment.

NFS file system objects have owners and permissions and NFS-application streamlining conforms to the file system permissions model by enforcing file server and volume policies. You must ensure that the policy is set correctly to Read-Only or Global Read-Write as appropriate. Setting the policy to Read-Only on a non-read-only file system results in Read-Only file system (ROFS) errors.

## To enable the NFS optimizer

1. Click the Setup tab to expand the Optimization Service menu.
1. Click Protocol: NFS to display the Optimization Service - Protocol: NFS page.

Figure 2-7. Optimization Service - Protocol: NFS Page



2. Use the controls to set NFS options, as described in the following table.

Control	Description
General	<b>Enable NFS Optimization.</b> Specify this option to enable NFS-application streamlining (optimization). You enable NFS-application optimization where NFS performance over the WAN is impacted by a high latency environment.
	<b>Enable NFS v2 and v4 Alarms.</b> Specify this option to enable alarm notification when v2 and v4 traffic is detected.
	<b>Default Server Policy.</b> Select one of the following options from the drop-down list to configure the default policy for NFS servers: <ul style="list-style-type: none"> <li>• <b>Global Read-Write.</b> Specifies a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the HP EFS WAN Accelerators) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.</li> <li>• <b>Custom.</b> Click <b>Custom</b> to display the <b>Enable Root Squashing</b> check box. Click <b>Enable Root Squashing</b> and <b>Apply</b> to enable the root squash feature for NFS volumes from this server. Root-squashing allows an NFS server to map any incoming user ID 0 or guest ID 0 to another number that does not have superuser privileges, often -2 (the nobody user).</li> <li>• <b>Home Directory.</b> All accesses to each directory are by a single user. This policy allows aggressive caching of data and metadata.</li> </ul>
	<b>Default Volume Policy.</b> Select one of the following options from the drop-down list to configure the default policy for NFS volumes: <ul style="list-style-type: none"> <li>• <b>Global Read-Write.</b> Specifies a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the HP EFS WAN Accelerators) and clients using other file protocols such as CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.</li> <li>• <b>Custom.</b> Click <b>Custom</b> to display the <b>Enable Root Squashing</b> check box. Click <b>Enable Root Squashing</b> and <b>Apply</b> to enable the root squash feature for NFS volumes from this server. Root-squashing allows an NFS server to map any incoming user ID 0 or guest ID 0 to another number that does not have superuser privileges, often -2 (the nobody user).</li> <li>• <b>Home Directory.</b> All accesses to each directory are by a single user. This policy allows aggressive caching of data and metadata.</li> </ul>
	<b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
Add New Server Configuration	<b>Name.</b> Specify the name of the server to add a new configuration for an NFS server.
	<b>Server IP.</b> Specify the IP address of the server and click <b>Add Server</b> .
	<b>Remove Selected Servers.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Servers</b> .

## Modifying NFS Server Settings

You can modify your NFS server configuration settings in the Setup: Optimization Service - Protocol: NFS Server <server name> page.

## To modify NFS server settings

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Protocol: NFS to display the Optimization Service - Protocol: NFS page.
3. Click the server name in the NFS Server list to display the Optimization Service - Protocol: NFS Server <server name> page.

**Figure 2-8. Optimization Service - Protocol: NFS Server <server name> Page**

[Home](#)
[Setup](#)
[Reports](#)
[Logging](#)
[Help](#)

Status: Healthy [ config save required ]

Logged in as: admin [ logout ]

- Optimization Service
  - General Settings
  - In-Path Rules
  - Protocol: CIFS
  - Protocol: MAPI
  - Protocol: MS-SQL
  - Protocol: NFS**
  - Protocol: HSTCP
  - Connection Pooling
  - Prepopulation
- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

- Configuration Manager
- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

### Optimization Service - Protocol: NFS Server blah

Configure your NFS server configuration for **blah**. [\[Return to Server List\]](#)

---

**Server Settings**

Server Policy: Global Read-Write

---

**Default Volume**

☐ Enable Default Volume with Policy: Global Read-Write

[Apply](#)

---

Configure the list of IP addresses assigned to this server.

**Server IP Address**

☐ 10.0.0.0

[Remove Selected IP Addresses](#)

**Add New IP Address:**

Server IP:

[Add IP Address](#)

---

We have detected that the following list of volumes are available on this server.

**Available Volume FSID Path**

*No NFS volumes available.*

---

The following NFS volume specific configurations override the default configurations above.

**Configured Volume FSID Policy** **Root Squash**

*No NFS volumes configured.*

[Remove Selected Volumes](#)

**Add New Volume Configuration:**

FSID:

Policy: Custom

☐ Enable Root Squash

[Add Volume](#)

---

[Save](#) [Reset](#)



## 4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Server Settings	<p><b>Server Policy.</b> Select one of the following options from the drop-down list to configure the default policy for NFS servers:</p> <ul style="list-style-type: none"> <li>• <b>Global Read-Write.</b> Specifies a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the HP EFS WAN Accelerators) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.</li> <li>• <b>Custom.</b> Enables you to turn on or off the root squash feature for NFS volumes from this server.</li> <li>• <b>Home Directory.</b> All accesses to each directory are by a single user. This policy allows aggressive caching of data and metadata.</li> </ul> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)</p>
Default Volume	<p><b>Enable Default Volume with Policy.</b> Specify this option and select one of the following options from the drop-down list to configure the default policy for NFS volumes:</p> <ul style="list-style-type: none"> <li>• <b>Global Read-Write.</b> Specifies a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the HP EFS WAN Accelerators) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.</li> <li>• <b>Custom.</b> Enables you to turn on or off the root squash feature for NFS volumes from this server.</li> <li>• <b>Home Directory.</b> All accesses to each directory are by a single user. This policy allows aggressive caching of data and metadata.</li> </ul> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)</p>
Add New Server Configuration	<p><b>Name.</b> Specify the name of the server to add a new configuration for an NFS server.</p> <p><b>Server IP.</b> Specify the IP address of the server and click <b>Add Server</b>.</p> <p><b>Remove Selected Servers.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Servers</b>.</p>

Control	Description
Add New Volume Configuration	<p><b>FSID.</b> Specify the file system identification number (ID) to add a new NFS volume.</p> <hr/> <p><b>Policy.</b> Select one of the following options from the drop-down list to configure the policy for NFS volumes:</p> <ul style="list-style-type: none"> <li>• <b>Global Read-Write.</b> Specifies a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the HP EFS WAN Accelerators) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.</li> <li>• <b>Custom.</b> Enables you to turn on or off the root squash feature for NFS volumes from this server.</li> <li>• <b>Home Directory.</b> All accesses to each directory are by a single user. This policy allows aggressive caching of data and metadata.</li> </ul> <hr/> <p><b>Enable Root Squash.</b> Select this option to enable root squashing.</p> <hr/> <p><b>Add Volume.</b> Click <b>Add Volume</b> to add the NFS volume to the list.</p> <hr/> <p><b>Remove Selected Volumes.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Volumes</b>.</p>

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling HSTCP Protocol Options

You enable the High Speed Transmission Control Protocol (HSTCP) in the Optimization Service - Protocol: HSTCP page.

HSTCP provides acceleration and high throughput for high bandwidth networks where the WAN pipe is large but latency is high. HSTCP is activated for all connections that have a Bandwidth-Delay Product (BDP) larger than 100 packets. HSTCP is available only on the Series 5000.

To configure HSTCP you must perform the following tasks.

Task	Description
Enable HSTCP support.	For detailed information, see <a href="#">“To enable HSTCP protocol support” on page 43</a> .
Increase the WAN buffers.	<p>Increase the WAN buffers to 2 Bandwidth Delay Product (BDP) or 10 MB. For detailed information, see <a href="#">“To enable HSTCP protocol support” on page 43</a>.</p> <p>You can calculate the BDP WAN buffer size. For example, for a link of 155 Mbps and 100 ms round-trip delay, the WAN buffers should be set to:</p> $2 * 155 \text{ Mbps} * 100 \text{ ms} = 3875000 \text{ bytes}$
Increase the LAN buffers.	Increase the LAN buffers to 1 MB. For detailed information, see <a href="#">“To enable HSTCP protocol support” on page 43</a> .

Task	Description
Enable in-path support.	For detailed information, see <a href="#">“Enabling In-Path and Out-of-Path Support” on page 22.</a>
Disable the Lempel-Ziv (LZ) compression and SDR in in-path optimization policies.	For detailed information about optimization policies if your WAN link capacity is 100 Mbps, see <a href="#">“Setting In-Path Rules” on page 25.</a>  With SDR enabled your throughput will bottleneck between 100 and 150 Mbps, which cancels out the benefit of HSTCP. If you have an Optical Carrier-3 line or faster, turning off SDR makes sense and allows HSTCP to reach its full potential. For a 2 Mbps link, regardless of the amount of latency, it is better to keep SDR enabled, because the HSTCP mechanism is typically not triggered until you reach beyond 100 Mbps of WAN throughput.

## To enable HSTCP protocol support

1. Click the Setup tab to expand the Optimization Service menu.

1. Click Protocol: HSTCP to display the Optimization Service - Protocol: HSTCP page.

**Figure 2-9.** Optimization Service - Protocol: HSTCP Page

The screenshot shows the HP StorageWorks EFS WAN Accelerator Management Console. The top navigation bar includes links for Home, Setup, Reports, Logging, and Help. The status is shown as 'Healthy' with a note '[config save required]'. The user is logged in as 'admin' with a 'logout' link. The left sidebar contains a menu for 'Optimization Service' with sub-items: General Settings, In-Path Rules, Protocol: CIFS, Protocol: MAPI, Protocol: MS-SQL, Protocol: NFS, Protocol: HSTCP (selected), Connection Pooling, Prepopulation, Host Settings, Advanced Networking, Proxy File Service, Port Labels, Reports, Logging, Date & Time, Authentication, Licenses, and Scheduled Jobs. The main content area is titled 'Optimization Service - Protocol: HSTCP' and includes a message: 'Check and modify your High Speed TCP protocol settings.' Below this, the 'High Speed TCP' section has a checkbox for 'Enable High Speed TCP' which is currently unchecked. To the right of the checkbox are four input fields for buffer sizes: LAN Send Buffer Size (81920 bytes), LAN Receive Buffer Size (32768 bytes), WAN Default Send Buffer Size (262140 bytes), and WAN Default Receive Buffer Size (262140 bytes). At the bottom right of the main content area are three buttons: Apply, Save, and Reset.

2. Use the controls to set HSTCP options, as described in the following table.

Control	Description
High-Speed TCP	<p><b>Enable High Speed TCP.</b> Select this option to enable HSTCP:</p> <ul style="list-style-type: none"><li>• <b>LAN Send Buffer Size.</b> Specify the send buffer size to set the buffer size used to send data out of the LAN. The default value is <b>81920</b>.</li><li>• <b>LAN Receive Buffer Size.</b> Specify the receive buffer size to set the buffer size used to receive data from the LAN. The default value is <b>32768</b>.</li><li>• <b>WAN Default Send Buffer Size.</b> Specify the send buffer size to set the buffer size used to send data out the WAN. The default value is <b>262140</b>.</li><li>• <b>WAN Default Receive Buffer Size.</b> Specify the receive buffer size to set the buffer size used to receive data from the WAN. The default value is <b>262140</b>.</li></ul>

3. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling Connection Pooling

You configure connection pooling in the Optimization Service - Connection Pooling page.

Connection pooling enhances network performance by reusing active connections instead of creating a new connection for every request. A connection pool manager maintains a pool of open connections. When a new connection request comes in, the pool manager checks if the pool contains unused connections and returns one if available. If all connections currently in the pool are busy and the maximum pool size has not been reached, the new connection is created and added to the pool. When the pool reaches its maximum size all new connection requests are queued up until a connection in the pool becomes available or the connection attempt times out.

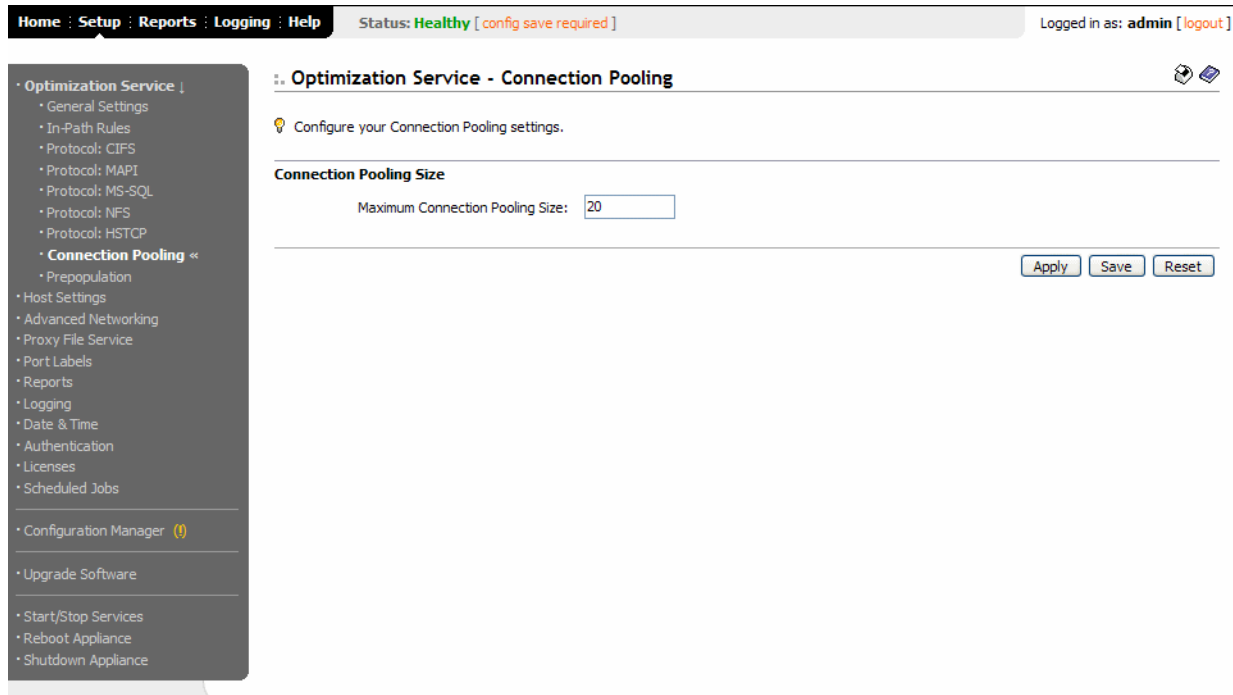
Connection pooling is useful for protocols which open a large number of short lived connections, such as HTTP.

Enabling this feature is *optional*.

## To enable connection pooling

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Connection Pooling to display the Optimization Service - Connection Pooling page.

Figure 2-10. Optimization Service - Connection Pooling Page



3. Under Connection Pooling Size, type the connection pooling size in the **Maximum Connection Pooling Size** text box. The default value is **20**.

---

**TIP:** To help you determine whether to modify the default, display the Connection Pooling report, described in [“Viewing Connection Pooling” on page 174](#). If the report indicates an unacceptably low ratio of pool hits per total connection requests, increase the pool size.

---

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

---

**IMPORTANT:** You must restart the HP EFS WAN Accelerator service on the HP EFS WAN Accelerator if you have modified your connection pooling parameters. For detailed information about restarting the HP EFS WAN Accelerator service, see the [“Starting and Stopping Services” on page 144](#).

---

## Enabling Transparent Prepopulation

You can enable or disable transparent prepopulation in the Optimization Service - Prepopulation Settings and Shares page.

With transparent prepopulation the HP EFS WAN Accelerator *warms* the data store with data from the client. When a data store is warm, the HP EFS WAN Accelerator has already seen the data. When data is sent again over the WAN only new or modified data is sent, dramatically increasing the rate of data transfer over the WAN.

After you enable transparent prepopulation you create a share on a remote file server.

### To enable prepopulation settings

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Prepopulation to display the Optimization Service - Prepopulation Settings and Shares page.
3. Click **Enable** to display the Prepopulation controls.

**Figure 2-11.** Optimization Service - Prepopulation Settings and Shares Page

Home : Setup : Reports : Logging : Help    Status: **Healthy**    Logged in as: admin [logout]

**Prepopulation Settings and Shares**

Enable or disable the Prepopulation Service and check or modify your Prepopulation shares.

**Enable Prepopulation Service**

Status: Prepopulation Service Enabled    [Disable](#)    [Enable](#)

**Transparent Prepopulation Using RCU**

☒ Enable Transparent Prepopulation Support    [Apply](#)    [Save](#)    [Reset](#)

**Prepopulation Shares**

Remote Path:

Account:

Password:

Password Confirm:

Comment (optional):

Sync Schedule, Date and Time:  (YYYY/MM/DD)  (HH:MM:SS)

Sync Interval:  Minutes

[Cancel](#)    [Save](#)

Remote Path	Comment	Syncing	Status	Actions
<a href="#">\\mint\main\pubs</a>	test	no	Share has error	-- Actions --

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add a Prepopulation Share	<b>Enable/Disable.</b> Click <b>Enable</b> to enable prepopulation on the share; click <b>Disable</b> to disable prepopulation on the share.
Transparent Prepopulation Using the RCU	<p><b>Enable Transparent Pre-population Support.</b> Specify this option to enable transparent pre-population using the HP Copy Utility (RCU).</p> <p>To enable transparent pre-population using the RCU, you must install and run the RCU on the client and server. Because the data has already been copied to the client and server, the HP EFS WAN Accelerator only copies new data, increasing optimization of traffic across the WAN. The RCU is available for download from the HP Technical Support site at <a href="http://www.hp.com">http://www.hp.com</a>.</p> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)</p> <p><b>Save.</b> Click <b>Save</b> to save your settings permanently or click <b>Reset</b> to return the settings to their previous values.</p>
Prepopulation Shares	<p><b>Remote Path.</b> The path to the data on the origin server or the Universal Naming Convention (UNC) path of a share to which you want to make available for prepopulation. For example, <code>\\&lt;origin-file-server&gt;\&lt;local-name&gt;</code></p> <p><b>NOTE:</b> Do not use guest or anonymous access to a Samba share. Also, the share and the origin-server share name cannot contain Unicode characters. The Management Console does not support Unicode characters.</p> <p><b>Account.</b> The local administrator account used to manage prepopulation shares.</p> <p><b>Password/Password Confirm.</b> Specify a password. You must use the correct syntax for the administrator login name (for example: <code>admin_user@parent_realm</code>) even if you belong to a subdomain.</p> <p><b>Comment.</b> Specify comments to help you identify the share.</p> <p><b>Sync Schedule Date and Time.</b> Specify a date and time to schedule synchronization of prepopulation shares with the HP EFS WAN Accelerator. The share conducts automatic synchronization with the origin server based on the synchronization interval.</p> <p>The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.</p> <p><b>Sync Interval.</b> Interval of updates (synchronization) in minutes. After the initial synchronization, the HP EFS WAN Accelerator retrieves data from the server at every synchronization interval. In these subsequent synchronizations, only new data that was modified or created after the previous synchronization is sent from file server to HP EFS WAN Accelerator.</p>

5. Click **Save** to save your settings permanently or click **Cancel** to return the settings to their previous values.

## Enabling and Synchronizing Prepopulation Shares

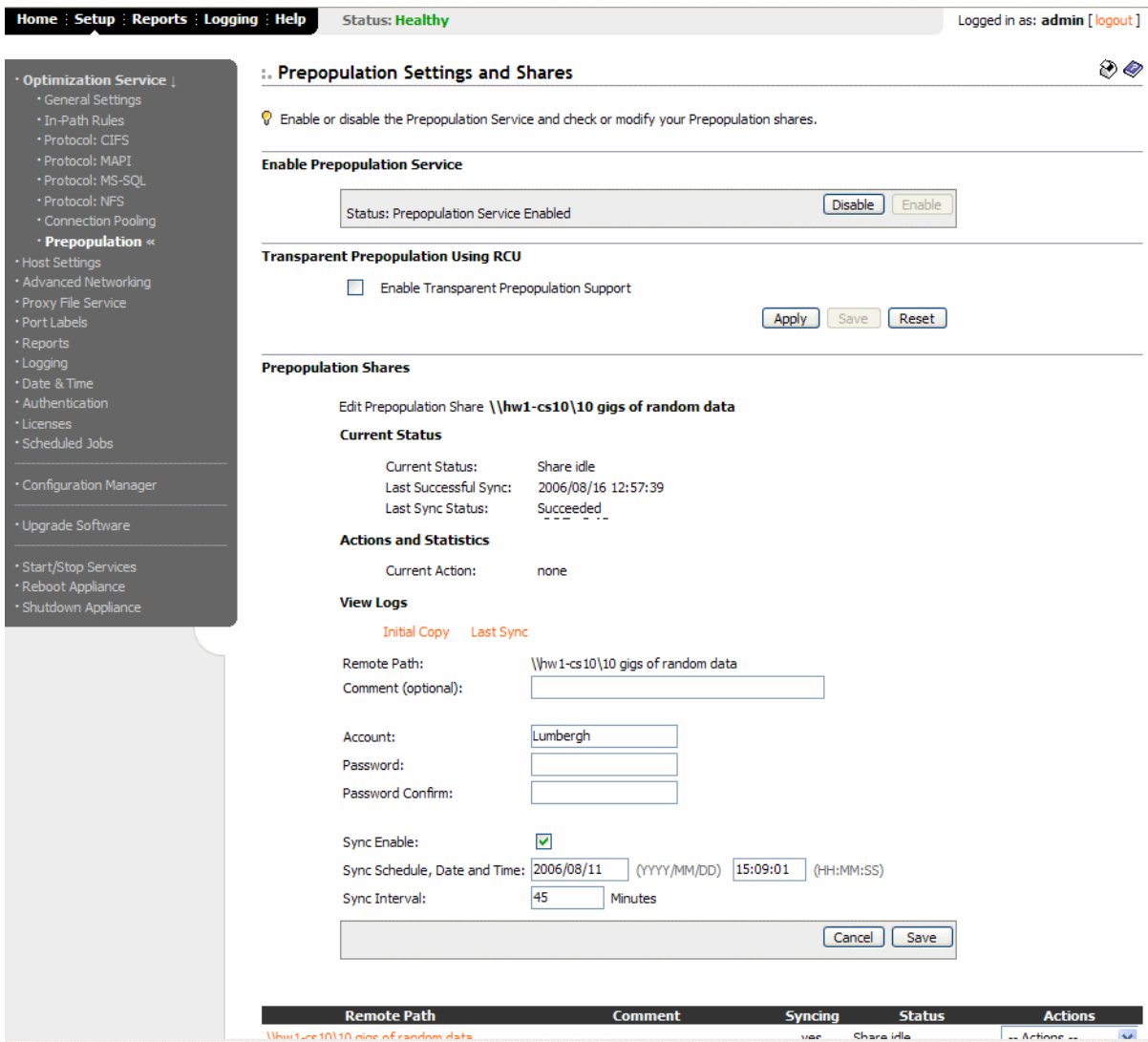
After you have configured your prepopulation shares, you must perform the initial synchronization of your shares in the Prepopulation Settings and Shares page.

When you perform the initial synchronization of the share, a copy of the data is downloaded from the origin server to the HP EFS WAN Accelerator. The HP EFS WAN Accelerator also configures the share for automatic synchronization according to the parameters you specified previously.

**To initialize and enable a prepopulation share**

1. Click the Setup tab to display the Optimization menu.
2. Click to Prepopulation to display the Prepopulation Settings and Shares page.
3. Click the Remote Path of the share that you want to initialize in the Prepopulation Shares list to display the Prepopulation Settings and Shares Details page.

**Figure 2-12.** Prepopulation Settings and Shares Details Page



4. Click **Syncing Enable** to download the initial copy of the share from the origin server to the HP EFS WAN Accelerator.
5. Click **Save** to write your changes to disk or **Cancel** to cancel your settings.



**NOTE:** When performing the initial synchronization, or when changing large amounts of data, your bandwidth utilization and other graphs may show pockets of inactivity. This is by design.

## Modifying Prepopulation Share Settings

### To modify prepopulation share settings

You can modify your prepopulation share settings in the Prepopulation Settings and Shares Details page.

1. Click the Setup tab to expand the Optimization menu.
2. Click Prepopulation to display the Prepopulation Settings and Shares page.
3. Click the Remote Path name in the Prepopulation shares list name that you want to modify to display the Prepopulation Settings and Shares page Details page.

**Figure 2-13.** Prepopulation Settings and Shares Details Page

- Optimization Service
  - General Settings
  - In-Path Rules
  - Protocol: CIFS
  - Protocol: MAP1
  - Protocol: MS-SQL
  - Protocol: NFS
  - Connection Pooling
- Prepopulation «
- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs
- Configuration Manager
- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

### Prepopulation Settings and Shares

Enable or disable the Prepopulation Service and check or modify your Prepopulation shares.

**Enable Prepopulation Service**

Status: Prepopulation Service Enabled

Disable

Enable

**Transparent Prepopulation Using RCU**

☐ Enable Transparent Prepopulation Support

Apply

Save

Reset

**Prepopulation Shares**

Edit Prepopulation Share \\hw1-cs10\10 gigs of random data

**Current Status**

Current Status: Share idle  
Last Successful Sync: 2006/08/16 12:57:39  
Last Sync Status: Succeeded

**Actions and Statistics**

Current Action: none

**View Logs**

Initial Copy   Last Sync

Remote Path: \\hw1-cs10\10 gigs of random data  
Comment (optional):  
Account: Lumbergh  
Password:  
Password Confirm:  
Sync Enable: ☒  
Sync Schedule, Date and Time: 2006/08/11 (YYYY/MM/DD) 15:09:01 (HH:MM:SS)  
Sync Interval: 45 Minutes

Cancel

Save

Remote Path	Comment	Syncing	Status	Actions
\\hw1-cs10\10 gigs of random data		yes	Share idle	Actions

4. Use the controls to modify your values.

Control	Description
Remote Path	<p>Specify the remote path of the origin file server where the share resides. You must use the Uniform Naming Convention (UNC) for the mapped drive for Version 3 shares. For example, \\&lt;origin-file-server&gt;\&lt;local-name&gt;</p> <p><b>IMPORTANT:</b> The prepopulation share and the origin-server share name cannot contain Unicode characters. The Management Console does not support Unicode characters.</p>
Comment	Optionally, specify a comment to help you identify the share.
Account	<p>Specify the login to be used to access the shares folder on the origin file server.</p> <p><b>IMPORTANT:</b> Make sure the users are members of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).</p>
Password/Password Confirm	Specify and confirm the password to be used to access the shares folder on the origin file server.
Sync Enable	Enables a download the initial copy of the share from the origin server to the HP EFS WAN Accelerator and configure the share for automatic synchronization.
Sync Schedule, Data and Time	<p>Specify the date and time that you want updates (synchronization) to start. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.</p> <p><b>IMPORTANT:</b> For local mode, changes are synchronized from the HP EFS WAN Accelerator to the origin file server; broadcast mode changes are synchronized from the origin file server to the HP EFS WAN Accelerator.</p>
Incremental Sync Interval	Specify the frequency of updates (synchronization) in minutes.
Full Sync Schedule, Date and Time	Specify the date and time that you want updates to start. Use full synchronization if performance is not an issue. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.
Full Sync Interval	Specify the frequency of updates (synchronization) in minutes.

5. Click **Save** to save your settings permanently or click **Cancel** to cancel your settings.

## Performing Manual Actions on Prepopulation Shares

You can verify a prepopulation share, perform a full synchronization, cancel an operation, or delete a prepopulation share in the Prepopulation Shares list. The shares list appears on the Prepopulation Settings and Shares Details page.

To perform manual actions on prepopulation shares

1. Click the Setup tab to expand the Optimization menu.
2. Click Prepopulation to display the Prepopulation Settings and Shares page.
3. Click the Remote Path name in the Prepopulation shares list name that you want to modify to display the Prepopulation Settings and Shares Details page.

Figure 2-14. Prepopulation Settings and Shares Details Page

• Optimization Service ▾

- General Settings
- In-Path Rules
- Protocol: CIFS
- Protocol: MAPI
- Protocol: MS-SQL
- Protocol: NFS
- Connection Pooling
- **Prepopulation** «

- Host Settings
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

- Configuration Manager
- Upgrade Software

- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

Prepopulation Settings and Shares

Enable or disable the Prepopulation Service and check or modify your Prepopulation shares.

Enable Prepopulation Service

Status: Prepopulation Service Enabled

DisableEnable

Transparent Prepopulation Using RCU

☐ Enable Transparent Prepopulation Support

ApplySaveReset

Prepopulation Shares

Edit Prepopulation Share \\hw1-cs10\10 gigs of random data

Current Status

Current Status:

Share idle

Last Successful Sync:

2006/08/16 12:57:39

Last Sync Status:

Succeeded

Actions and Statistics

Current Action:

none

View Logs

Initial Copy

Last Sync

Remote Path:

\\hw1-cs10\10 gigs of random data

Comment (optional):

Account:

Lumbergh

Password:

Password Confirm:

Sync Enable:

☒

Sync Schedule, Date and Time:

2006/08/11 (YYYY/MM/DD)

15:09:01 (HH:MM:SS)

Sync Interval:

45

Minutes

Cancel

Save

4. Select one of the following actions for the prepopulation share, as described in the following table.

Control	Description
Actions	Select one of the following actions from the drop-down list: <ul style="list-style-type: none"><li>• <b>Start Full Sync.</b> Allows you to immediately synchronize the share and its corresponding remote share on the origin file server. You may select <b>Start Full Sync</b> at any time to manually synchronize a share.</li><li>• <b>Cancel Action.</b> Cancels the synchronization process.</li><li>• <b>Delete Share.</b> Deletes the selected share.</li></ul>

---

## Setting Host Parameters

This section describes how to set host parameters for the HP EFS WAN Accelerator. It includes the following sections:

- ◆ [“Setting the Primary Interface,” next](#)
- ◆ [“Setting In-Path Interfaces” on page 54](#)
- ◆ [“Setting Auxiliary Interfaces” on page 58](#)
- ◆ [“Setting Main Static Routes” on page 59](#)
- ◆ [“Setting Static In-Path Routes” on page 60](#)
- ◆ [“Setting the DNS” on page 61](#)
- ◆ [“Modifying the Host Name” on page 63](#)
- ◆ [“Mapping Hosts to IP Addresses” on page 63](#)
- ◆ [“Setting Proxies” on page 64](#)

### Setting the Primary Interface

You modify settings for the primary interface in the Host Settings - Interface Primary page.

You were prompted to configure the primary interface when you completed the installation wizard. This section describes how you can modify these settings.

---

**IMPORTANT:** The primary and in-path interfaces can share the same subnet. The primary and auxiliary interfaces cannot share the same network subnet.

---

### To set the primary interface

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to display the Host Settings - Interface: Primary page.

Figure 2-15. Host Settings - Interface Primary Page

Home
Setup
Reports
Logging
Help

Status: Healthy [config save required]
Logged in as: admin [logout]

- Optimization Service
- Host Settings
  - Interface: Primary «
  - Interface: In-Path
  - Interface: AUX
  - Routing: Main
  - Routing: In-Path
  - DNS Settings
  - Hostname
  - Hosts
  - Proxies
- Advanced Networking
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs
- Configuration Manager (?)
- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

Host Settings - Interface: Primary

Configure your primary interface settings.

IP Address

☐ Obtain IP Address Automatically
☒ Specify IP Address Manually

IP Address:

10.11.34.6

Subnet Mask:

255.255.0.0

Primary Gateway IP:

10.0.0.1

Additional Interface Settings

Speed:

Auto

UNKNOWN

Duplex:

Auto

UNKNOWN

MTU:

1500

Apply

Save

Reset

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
IP Address	<b>Obtain IP address automatically.</b> Specify this option to automatically obtain the IP address from a Dynamic Host Configuration Protocol DHCP server. (A DHCP server must be available so that the HP EFS WAN Accelerator can request the IP address from it.)
	<b>IMPORTANT:</b> The primary and in-path interfaces can share the same subnet. The primary and auxiliary interfaces cannot share the same network subnet.
	<b>Specify IP Address Manually.</b> Specify this option if you do not use a DHCP server to set the IP address. Specify the following settings: <ul style="list-style-type: none"> <li>• <b>IP Address.</b> Specify an IP address.</li> <li>• <b>Subnet Mask.</b> Specify a subnet mask.</li> <li>• <b>Primary Gateway.</b> Specify the primary gateway IP address. The primary gateway must be in the same network as the primary interface. You must set the primary gateway for in-path configurations.</li></ul>

Control	Description
Additional Interface Settings	<p><b>Speed.</b> Select the speed from the drop-down list. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same speed settings.</p> <hr/> <p><b>Duplex.</b> Select <b>Auto</b>, <b>Full</b> or <b>Half</b> from the drop-down list. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same duplex settings.</p> <hr/> <p><b>MTU.</b> Specify the Maximum Transmission Unit (MTU) value. The MTU is the largest physical packet size, measured in Bytes, that a network can transmit. The default value is <b>1500</b>.</p>

- Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous value.

## Setting In-Path Interfaces

You modify the settings for the in-path interface in the Host Settings - Interface: In-Path (LAN/WAN) page.

You specify the in-path interface if you plan to have the appliance in the direct path (the same subnet) as the client and the server in your network. You also set the in-path gateway (WAN router).

---

**NOTE:** You were prompted to configure the in-path interface when you completed the installation wizard. This section describes how you can modify these settings.

---

## Speed and Duplex Tips

If your network routers do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the in-path interface (that is, the HP EFS WAN Accelerator).

Speed and duplex mismatches can easily occur in a network. For example, if one end of the link is set at **half** or **full-duplex** and the other end of the link is configured to auto negotiate (**auto**), the link defaults to **half-duplex**, regardless of the duplex setting on the non-auto-negotiated end. This duplex mismatch passes traffic, but it causes interface errors and results in degraded optimization.

The following are general guidelines to avoid speed and duplex mismatches when configuring the HP EFS WAN Accelerator:

- ◆ Routers are often configured with fixed speed and duplex settings. Check your router configuration and set it to match the HP EFS WAN Accelerator WAN and LAN settings. Make sure your switch has the correct setting.
- ◆ After you finish configuring the HP EFS WAN Accelerator, check for speed and duplex error messages (**crc** or **frame** errors) in the Logging, View System Log page of the Management Console. For detailed information about viewing HP EFS WAN Accelerator logs, see “[Viewing HP EFS WAN Accelerator Logs](#)” on [page 201](#).
- ◆ If there is a serious problem with the HP EFS WAN Accelerator and it goes into bypass mode (that is, it automatically continues to pass traffic through your network), a speed and duplex mismatch might occur when you reboot the HP EFS WAN Accelerator. To avoid a speed and duplex mismatch, configure your LAN external pair to match the WAN external pair. For example, **auto** on the LAN and WAN and fixed to **100 FULL** on the LAN and WAN.

### To set the in-path interface

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click Interface: In-Path to display the Host Settings - Interface: In-Path (LAN/WAN) page.

**Figure 2-16.** Host Settings - Interface: In-Path (LAN/WAN) Page

The screenshot shows the HP StorageWorks EFS WAN Accelerator Management Console. The top navigation bar includes links for Home, Setup, Reports, Logging, and Help. The status bar indicates the system is Healthy, with a note that a config save is required. The user is logged in as admin. The left sidebar shows a tree view of the configuration options, with Host Settings expanded and Interface: In-Path selected. The main content area is titled 'Host Settings - Interface: In-Path (LAN/WAN)' and contains a warning icon and text: 'Configure your in-path interface settings. This is the in-path main interface.' Below this, the 'IP Address' section has two radio buttons: 'Obtain IP Address Automatically' (unselected) and 'Specify IP Address Manually' (selected). The manual configuration fields show IP Address: 10.11.62.87, Subnet Mask: 255.255.0.0, and In-Path Gateway IP: (empty). The 'Additional Interface Settings' section includes dropdown menus for LAN Speed (Auto), Duplex (Auto), WAN Speed (Auto), and Duplex (Auto), each with a corresponding value in parentheses (1000Mb/s (auto), full (auto), 1000Mb/s (auto), full (auto)). There are also input fields for MTU (1500) and VLAN Tag ID (0), with a note that 0 is untagged. At the bottom right, there are buttons for Apply, Save, and Reset.

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
IP Address	<p><b>Obtain IP address automatically.</b> Specify this option to obtain the IP address from a DHCP server.</p> <p><b>IMPORTANT:</b> The primary and in-path interfaces can share the same subnet. The primary and auxiliary interfaces cannot share the same network subnet.</p> <hr/> <p><b>Specify IP Address Manually.</b> Specify this option if you do not use a DHCP server to set the IP address. Specify the following settings:</p> <ul style="list-style-type: none"><li>• <b>IP Address.</b> Specify an IP address. This IP address is the in-path main interface.</li><li>• <b>Subnet Mask.</b> Specify the subnet mask.</li><li>• <b>In-Path Gateway IP.</b> Specify the IP address for the in-path gateway. If you have a router (or a Layer-3 switch) on the LAN side of your network, specify this device as the in-path gateway.</li></ul> <p><b>IMPORTANT:</b> If there is a routed network on the LAN-side of the in-path appliance, the router that is the default gateway for the appliance must not have the Access Control List (ACL) configured to drop packets from the remote hosts as its source. The in-path appliance uses IP masquerading to appear as the remote server.</p>



Control	Description
Additional Interface Settings	<p><b>LAN Speed.</b> Select the speed from the drop-down list to set the speed for the in-path LAN port. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same settings.</p> <hr/> <p><b>Duplex.</b> Select <b>Auto</b>, <b>Full</b>, or <b>Half</b> from the drop-down list to set the duplex speed for the in-path LAN port. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same settings.</p> <hr/> <p><b>WAN Speed.</b> Select the speed from the drop-down list to set the speed for the in-path WAN port. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same settings.</p> <hr/> <p><b>Duplex.</b> Select <b>Auto</b>, <b>Full</b>, or <b>Half</b> from the drop-down list to set the duplex speed for the in-path WAN port. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must manually set the speed and duplex for the primary interface.</p> <p>The speed and duplex must match (LAN and WAN) in an in-path configuration. If they do not match you might have a large number of errors on the interface when it is in bypass mode, because the switch and router are not set with the same settings.</p> <hr/> <p><b>MTU.</b> Specify the Maximum Transmission Unit (MTU) value. The MTU is the largest physical packet size, measured in Bytes, that a network can transmit. The default value is <b>1500</b>.</p>
VLAN	<p><b>VLAN Tag ID.</b> If you have enabled VLAN tagging, type a numeric ID. Specify <b>0</b> to leave the interface untagged.</p> <p>When you specify the VLAN Tag ID for the in-path interface, all packets originating from the HP EFS WAN Accelerator are tagged with that identification number. This is the VLAN tag that the appliance uses to communicate with other HP EFS WAN Accelerators in your network. The VLAN Tag ID might be the same value or a different value than the VLAN tag used on the client. A zero (0) value specifies non-tagged (or native) VLAN.</p> <p><b>NOTE:</b> When the HP EFS WAN Accelerator communicates with a client or a server it uses the same VLAN tag as the client or the server. If the HP EFS WAN Accelerator cannot determine which VLAN the client or server is in, it uses its own VLAN until it is able to determine that information.</p> <p><b>NOTE:</b> You must also define in-path rules to apply to your VLANs. For detailed information, see <a href="#">“Setting In-Path Rules” on page 25</a>.</p>

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Auxiliary Interfaces

You set up an auxiliary interface, which provides support if your network has a dedicated management subnet, in the Host Settings - Interface: AUX page. For example, if your network has an auxiliary interface that connects and passes packets between the HP EFS WAN Accelerator and a different network, such as one purely for device management.

---

**IMPORTANT:** The primary and auxiliary interfaces cannot share the same network subnet. The auxiliary and in-path interfaces cannot share the same subnet.

---

Enabling this interface is *optional*.

### To set an auxiliary interface

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click Interface: AUX to display the Host Settings - Interface: AUX page.

**Figure 2-17.** Host Settings - Interface: AUX Page

The screenshot displays the 'Host Settings - Interface: AUX' configuration page. At the top, a navigation bar includes links for Home, Setup, Reports, Logging, and Help, along with a status indicator 'Healthy [config save required]' and a user login 'admin [logout]'. A left-hand sidebar lists various system settings, with 'Host Settings' expanded and 'Interface: AUX' selected. The main content area is titled 'Host Settings - Interface: AUX' and contains a lightbulb icon with the text 'Configure your AUX interface settings. This interface is used for dedicated management subnets only.' Below this, the 'AUX Interface' is set to 'Enabled' via a dropdown menu. The 'IP Address' section offers two options: 'Obtain IP Address Automatically' (unselected) and 'Specify IP Address Manually' (selected), with input fields for 'IP Address' and 'Subnet Mask'. The 'Additional Interface Settings' section includes 'Speed' (Auto), 'Duplex' (Auto), and 'MTU' (input field). At the bottom right, there are three buttons: 'Apply', 'Save', and 'Reset'.

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
AUX Interface Enabled	<p>Select <b>Enabled</b> or <b>Disabled</b> from the drop-down list.</p> <p><b>IMPORTANT:</b> The primary and auxiliary interfaces cannot share the same network subnet. The auxiliary and in-path interfaces cannot share the same subnet. You cannot use the auxiliary port for out-of-path HP EFS WAN Accelerators.</p>
IP Address	<p><b>Obtain IP address automatically.</b> Specify this option to obtain the IP address from a dynamic host configuration protocol (DHCP) server.</p> <p><b>Specify IP Address Manually.</b> Specify this option if you do not use a DHCP server to set the IP address. Specify the following settings:</p> <ul style="list-style-type: none"> <li>• <b>IP Address.</b> Specify an IP address.</li> <li>• <b>Subnet Mask.</b> Specify the subnet mask.</li> </ul>
Additional Interface Settings	<p><b>Speed.</b> Select the speed from the drop-down list to set the speed for the auxiliary interface. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must set the speed and duplex manually.</p> <p><b>Duplex.</b> Select <b>Auto</b>, <b>Full</b>, or <b>Half</b> from the drop-down list to set the duplex speed for the auxiliary interface. The default value is <b>Auto</b>.</p> <p>If your network routers or switches do not automatically negotiate the speed and duplex, you must set the speed and duplex manually.</p> <p><b>MTU.</b> Specify the Maximum Transmission Unit (MTU) value. The MTU is the largest physical packet size, measured in Bytes, that a network can transmit. The default is <b>1500</b>.</p>

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Main Static Routes

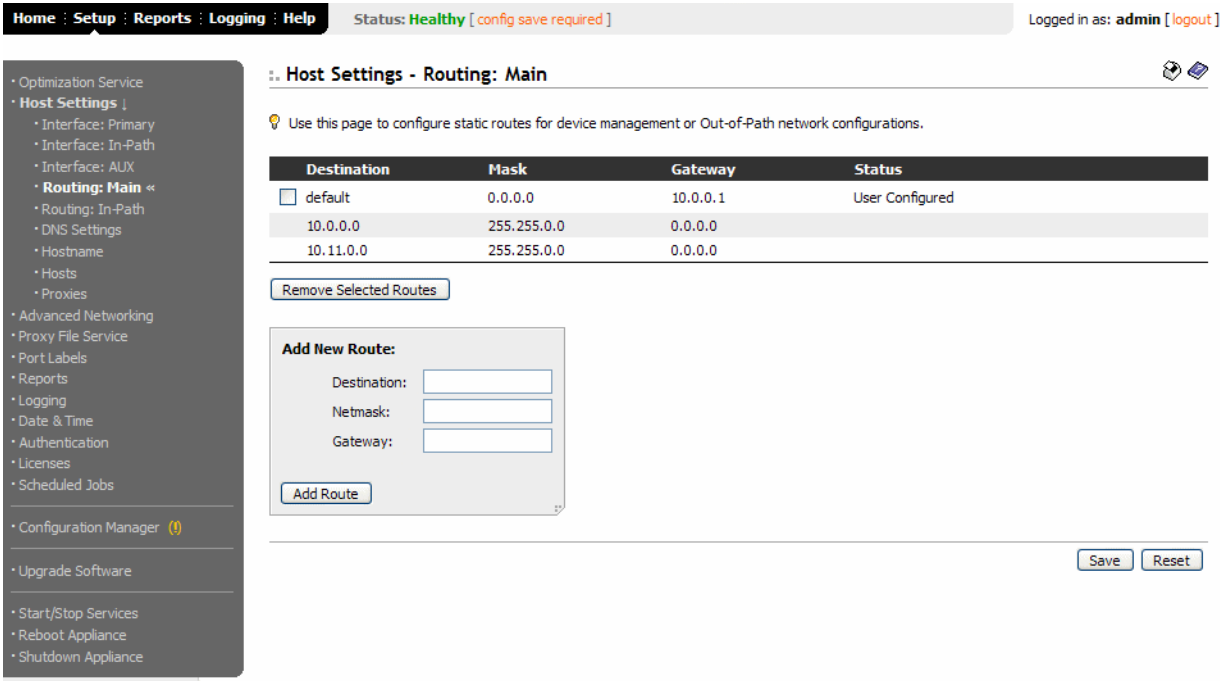
You set static routes for device management or out-of-path network configurations in the Host Settings - Routing: Main page.

Main static network routes set routing rules in the main routing table for the primary interface.

To set a static main route

- 1. Click the Setup tab to display the Setup menu.
- 2. Click Host Settings to expand the Host Settings menu.
- 3. Click Routing: Main to display Host Settings - Routing: Main page.

Figure 2-18. Host Settings - Routing: Main Page



- 4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Route	<b>Destination.</b> Specify the IP address.
	<b>Netmask.</b> Specify the subnet mask.
	<b>Gateway.</b> Specify the IP address for the gateway. The gateway must be in the same network as the primary or auxiliary interface.
	<b>Add Route.</b> Specify this option to add the entry to the list.
	<b>Remove Selected Routes.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Routes</b> .

- 5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

Setting Static In-Path Routes

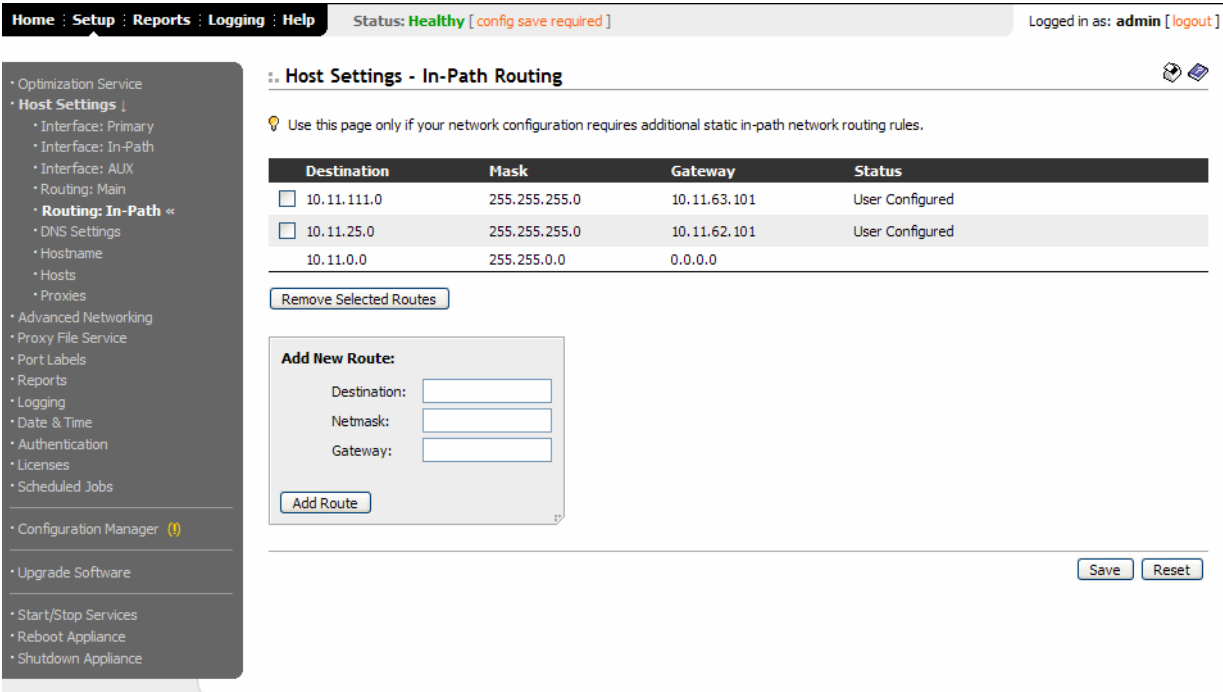
You configure static, in-path network routes if your network configuration requires additional static in-path network routing rules in the Host Settings - Routing: In-Path page.

The values you specify set the routing table for in-path interfaces (as opposed to the primary interface).

### To set a static, in-path route

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click Routing: In-Path to display the Host Settings - In-Path Routing page.

Figure 2-19. Host Settings - In-Path Routing Page



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Route	<b>Destination.</b> Specify the IP address.
	<b>Netmask.</b> Specify the subnet mask.
	<b>Gateway.</b> Specify the IP address for the gateway. The gateway must be in the same network as the primary or auxiliary interface.
	<b>Add Route.</b> Specify this option to add the entry to the list.
	<b>Remove Selected Routes.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Routes</b> .

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting the DNS

You set the primary Domain Name Service (DNS) server and domain for the HP EFS WAN Accelerator in the Host Settings - DNS Settings page.

HP recommends you use DNS.

**NOTE:** You were prompted to configure DNS when you completed the installation wizard. This section describes how you can modify these settings.

## To set the DNS server

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click DNS Settings to display the Host Settings - DNS Settings page.

**Figure 2-20.** Host Settings - DNS Settings Page

The screenshot shows the 'Host Settings - DNS Settings' page. The top navigation bar includes 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy' with a note '[ config save required ]'. The user is logged in as 'admin' with a 'logout' link. The left sidebar shows a tree view with 'Host Settings' expanded, and 'DNS Settings' selected. The main content area has a title 'Host Settings - DNS Settings' and a subtitle 'Configure your DNS settings.' Below this, there are two sections: 'Name Servers' and 'Domain Search'. The 'Name Servers' section has three input fields for 'Primary DNS IP', 'Secondary DNS IP', and 'Tertiary DNS IP', with a 'Set Name Servers' button below them. The 'Domain Search' section has a 'Domain(s):' list box containing 'nbttech.com', 'nbt.com', and 'riverbed.com', a 'Remove Selected Domain' button, and an 'Add Domain' section with an input field and an 'Add Domain' button. At the bottom right, there are 'Save' and 'Reset' buttons.

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Name Servers	<p>Set one or more of the following:</p> <ul style="list-style-type: none"><li>• <b>Primary DNS IP.</b> Specify the IP address for the primary name server.</li><li>• <b>Secondary DNS IP.</b> Optionally, specify the IP address for the secondary name server.</li><li>• <b>Tertiary DNS IP.</b> Optionally, specify the IP address for the tertiary name server.</li></ul> <p>To apply your settings, click <b>Set Name Servers</b>.</p>
Domain Search	<p><b>Add Domain.</b> Specify the domain name and click <b>Add Domain</b>. If you specify domains the HP EFS WAN Accelerator automatically finds the appropriate domain for each of the hosts that you enter in the system.</p> <p><b>Remove Selected Domain.</b> To remove an entry, click the box next to the domain name and click <b>Remove Selected Domain</b>.</p>

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying the Host Name

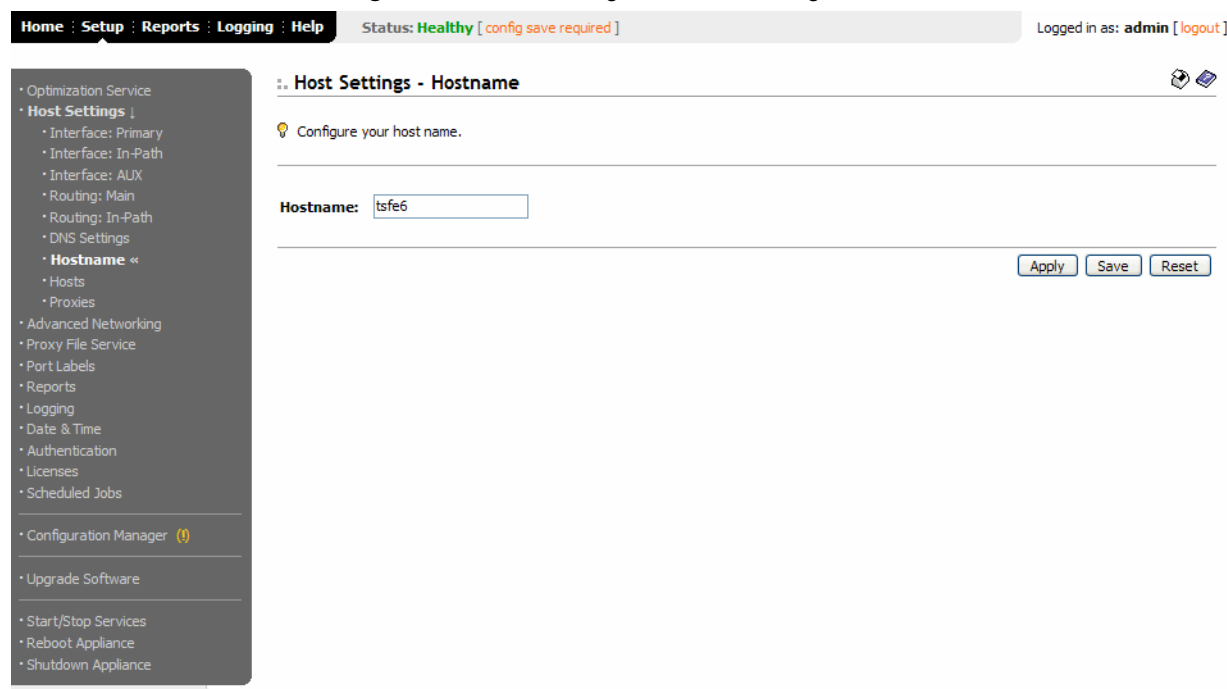
You can change the host name for the HP EFS WAN Accelerator in the Host Settings - Host Name page.

**NOTE:** You were prompted to specify a host name when you completed the installation wizard. This section describes how you can modify these settings.

### To modify the host name

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click Host Name to display the Host Settings - Host Name page.

**Figure 2-21.** Host Settings - Host Name Page



4. Modify the text in the **Host Name** text box to change the host name.
5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Mapping Hosts to IP Addresses

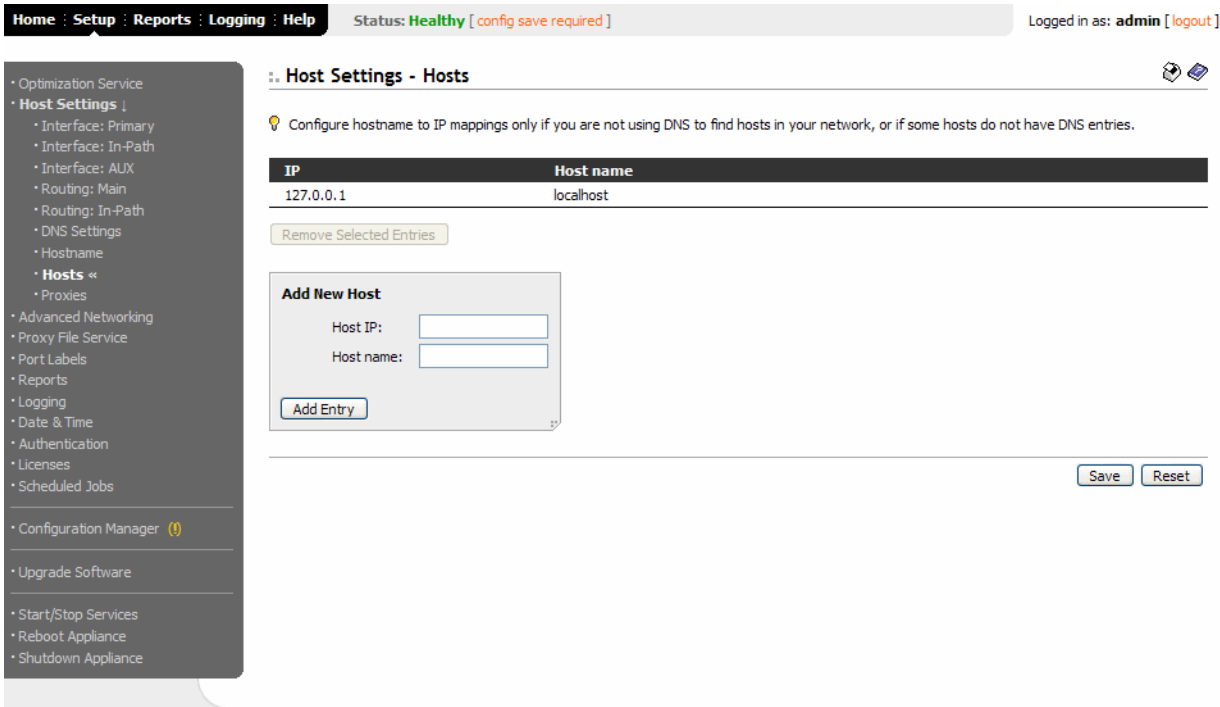
You can map a host name to IP addresses in the Host Settings - Hosts page.

Specify these values only if you are not using DNS to resolve host names and IP addresses in your system (or if the host does not have a DNS entry).

**To map a host name to an IP address**

- 1. Click the Setup tab to display the Setup menu.
- 2. Click Host Settings to expand the Host Settings menu.
- 3. Click Hosts to display the Host Settings - Hosts page.

**Figure 2-22.** Host Settings - Hosts Page



- 4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Host	<b>Host IP.</b> Specify the IP address for the host.
	<b>Host name.</b> Specify a host name.
	<b>Add Entry.</b> Click <b>Add Entry</b> to add a host and IP address.
	<b>Remove Selected Hosts.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Hosts</b> .

- 5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

**Setting Proxies**

You can specify a Web or FTP proxy in the Host Settings - Proxies page.

This proxy is used when a Uniform Resource Locator (URL) is specified in the Management Console or the CLI. For example, the proxy is used in the Software Upgrade page if you specify a URL from which to download the software image.

This setting applies only if you specify FTP or HTTP in the URL.



Setting proxies is *optional*.

### To enable a proxy

1. Click the Setup tab to display the Setup menu.
2. Click Host Settings to expand the Host Settings menu.
3. Click Proxies to display the Host Settings - Proxies page.

**Figure 2-23.** Host Settings - Proxies Page

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Web/FTP Proxy IP Address	Specify the IP address for the Web/FTP proxy.
Port	Specify the port number for the Web/FTP proxy.

5. Click **Apply** to apply your settings to the running configuration.
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Advanced Network Parameters

This section describes how to configure advanced network parameters in the HP EFS WAN Accelerator. It includes the following sections:

- ◆ “[Enabling Asymmetric Routing Auto-Detection,](#)” next

- ◆ [“Enabling Connection Forwarding” on page 68](#)
- ◆ [“Enabling Encryption” on page 70](#)
- ◆ [“Enabling Failover and Data Store Synchronization” on page 73](#)
- ◆ [“Setting Peering Rules” on page 79](#)
- ◆ [“Enabling Quality of Service” on page 81](#)
- ◆ [“Modifying a QoS Class” on page 85](#)
- ◆ [“Setting QoS Marking” on page 87](#)
- ◆ [“Modifying QoS Marking Descriptions” on page 89](#)
- ◆ [“Modifying Service Ports” on page 90](#)
- ◆ [“Enabling Simplified Routing” on page 92](#)
- ◆ [“Enabling WCCP Groups” on page 94](#)
- ◆ [“Modifying WCCP Group Settings” on page 96](#)

## Enabling Asymmetric Routing Auto-Detection

You enable asymmetric route auto-detection in the Advanced Networking - Asymmetric Routing page. Asymmetric route auto-detection detects and reports asymmetric routing conditions and caches this information to avoid losing connectivity between a client and a server.

When HP EFS WAN Accelerators are deployed in a network, all TCP traffic must flow through the same HP EFS WAN Accelerators in the forward and reverse direction. If traffic flows through an HP EFS WAN Accelerator in one direction and not the other, then TCP clients are unable to make connections to TCP servers. When deploying HP EFS WAN Accelerators into redundant networks, there is a possibility of traffic taking different forward and return paths so that traffic in one direction goes through HP EFS WAN Accelerators but traffic in the reverse direction does not.

If asymmetric routing is detected, the pair of IP addresses, defined by the client and server addresses of this connection, is cached on the HP EFS WAN Accelerator. Further connections between these hosts are not optimized until that particular asymmetric routing cache entry times out.

Detecting and caching asymmetric routes does not optimize these packets. If you want to optimize asymmetric routed packets you must make sure that packets going to the WAN always go through an HP EFS WAN Accelerator either by using a multi-port HP EFS WAN Accelerator, connection forwarding, or using external ways to redirect packets, such as WCCP or PBR.

For detailed information, see [“Enabling Connection Forwarding” on page 68](#) or the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

## To enable asymmetric routing auto-detection

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to display Advanced Networking - Asymmetric Routing page.

Figure 2-24. Advanced Networking - Asymmetric Routing Page

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
General Settings	<p><b>Enable Asymmetric Routing Detection.</b> Specify this option to detect asymmetric routes in your network.</p> <p><b>Enable Asymmetric Routing Caching.</b> Specify this option to enable the asymmetric routing cache in the HP EFS WAN Accelerator. If asymmetric routing is detected, the pair of IP addresses, defined by the client and server addresses of this connection, is cached on the HP EFS WAN Accelerator. Further connections between these hosts are not optimized until that particular asymmetric routing cache entry times out.</p> <p>Detecting and caching asymmetric routes does not optimize these packets. If you want to optimize asymmetric routed packets you must make sure that packets going to the WAN always go through an HP EFS WAN Accelerator either by using a multi-port HP EFS WAN Accelerator, connection forwarding, or using external ways to redirect packets, such as WCCP or PBR.</p> <p>For detailed information, see <a href="#">“Enabling Connection Forwarding” on page 68</a> or the <i>HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide</i>.</p> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.</p>
Source IP Table	<p><b>Remove Selected Entries.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Entries</b>.</p>

4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

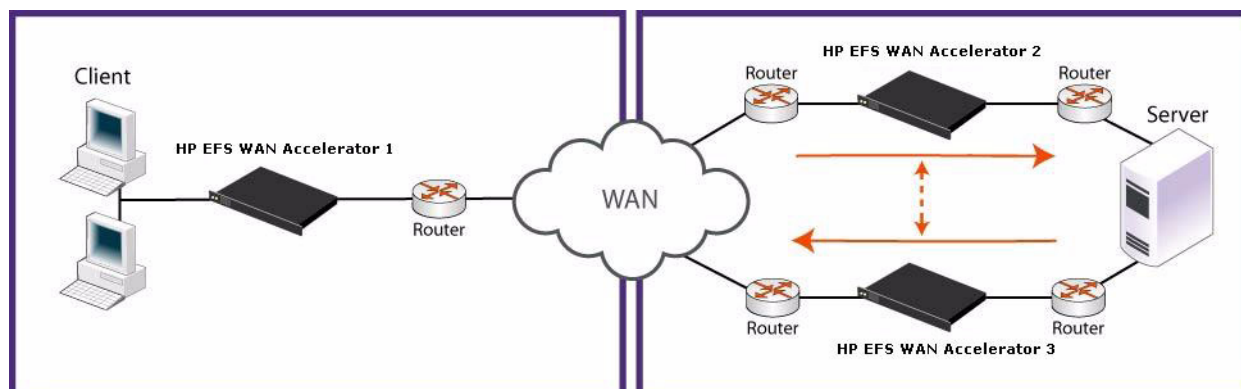
## Enabling Connection Forwarding

You enable connection forwarding in a network configuration with multiple paths from the server in the Advanced Networking - Connection Forwarding page.

You enable connection forwarding only in asymmetric networks; that is, in networks in which a client request traverses a different network path than the server response. The default port for connection forwarding is **7850**.

To optimize connections in asymmetric networks, packets traveling in both directions must pass through the same client-side and server-side HP EFS WAN Accelerator. If you have one path from the client to the server and a different path from the server to the client, you need to enable in-path connection forwarding and configure the HP EFS WAN Accelerators communicate with each other. These HP EFS WAN Accelerators are called neighbors and exchange connection information to redirect packets to each other.

**Figure 2-25.** Asymmetric Network



Neighbors can be placed in the same physical site or in different sites but the latency between them should be small because the packets travelling between them are not optimized.

---

**IMPORTANT:** When you define a neighbor, you specify the HP EFS WAN Accelerator in-path IP address, not the primary IP address.

---

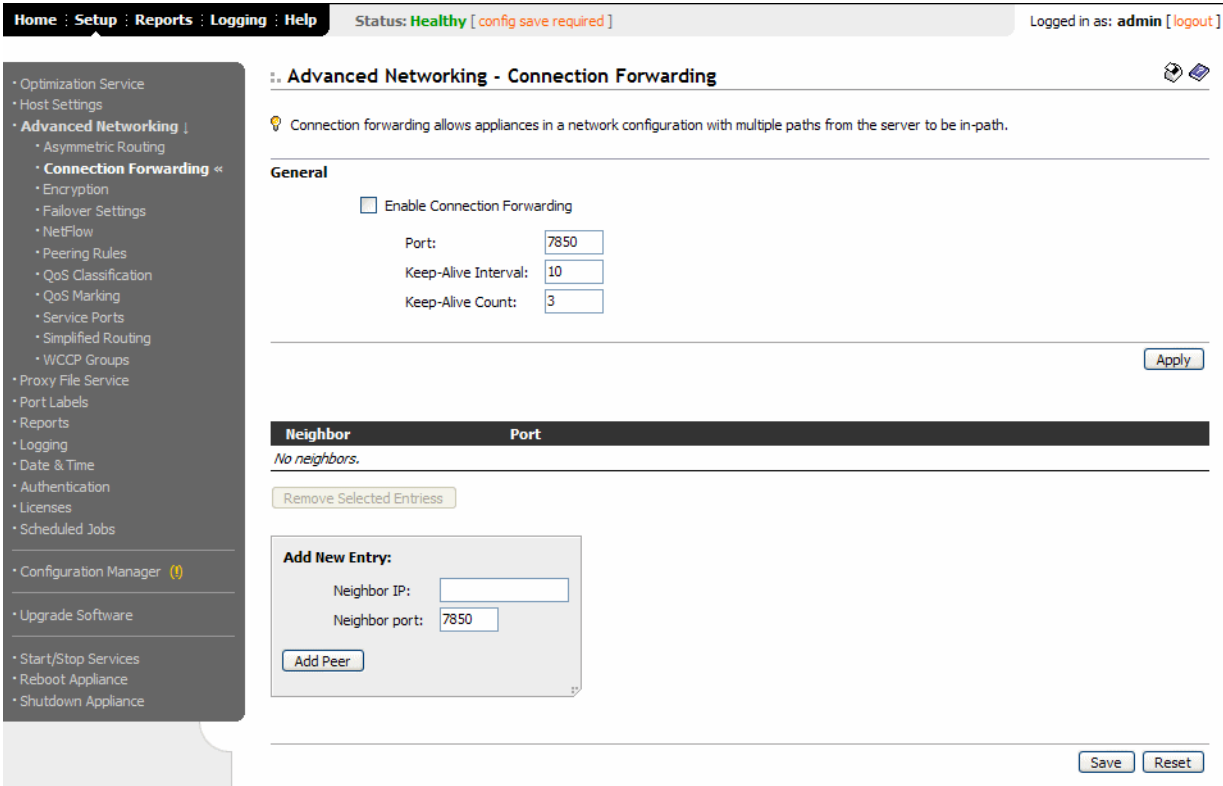
If there are more than two possible paths, additional HP EFS WAN Accelerators must be installed on each path and configured as neighbors. Neighbors are notified in parallel so that the delay introduced at connection set up is equal to the time it takes to get an acknowledgement from the furthest neighbor.

For detailed information about connection forwarding, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

To enable connection forwarding

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu and display the Advanced Networking -Connection Forwarding page.

Figure 2-26. Advanced Networking - Connection Forwarding Page



3. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<b>Enable Connection Forwarding.</b> Specify this option to enable connection forwarding by default on all neighbors added to the peer list. The default port for connection forwarding is <b>7850</b> .
	<b>Port.</b> Specify the port number to use as the default for neighbor appliance in-path port. The default is <b>7850</b> .
	<b>Keep-Alive Interval.</b> Specify the number of seconds to use as the default interval for <b>ping</b> commands between neighbor appliances.
	<b>Keep-Alive Count.</b> Specify the number of tries to use as the default number of failed <b>ping</b> attempts before an appliance terminates a connection with a neighbor. The default value is <b>3</b> .
	<b>Apply.</b> Click <b>Apply</b> to apply them to entries in the peer list.

Control	Description
Add New Entry	<p><b>Neighbor IP.</b> Specify the in-path IP address for the neighbor appliance. When you define a neighbor, you must specify the appliance in-path IP address, not the primary IP address.</p> <p><b>Neighbor Port.</b> Specify the in-path port for the neighbor appliance. The default is <b>7850</b>.</p> <p><b>Add Peer.</b> Click <b>Add Peer</b> to add a neighbor to the peer list.</p> <p><b>Remove Selected Entries.</b> To remove an entry, select it and click <b>Remove Selected Entries</b>.</p>

4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling Encryption

You configure IP Security Protocol (IPsec) encryption to allow data to be communicated securely between peer HP EFS WAN Accelerators in the Advanced Networking - Encryption page.

Enabling IPsec encryption makes it difficult for a third party to view your data or pose as a machine you expect to receive data from. To enable IPsec, you must specify at least one encryption and authentication algorithm. Only optimized data is protected, pass-through traffic is not.

Enabling IPsec support is *optional*.

---

**IMPORTANT:** You must set IPsec support on each peer HP EFS WAN Accelerator in your network for which you want to establish a secure connection. You must also specify a shared secret on each peer HP EFS WAN Accelerator.

---



---

**NOTE:** If you Network Address Translate (NAT) traffic between HP EFS WAN Accelerators, you cannot use the IPSEC channel between the appliances because the NAT changes the packet headers causing IPSEC to reject them.

---

## To enable encryption

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click Encryption to display the Advanced Networking - Encryption page.

Figure 2-27. Advanced Networking - Encryption Page

[Home](#) : [Setup](#) : [Reports](#) : [Logging](#) : [Help](#)

Status: **Healthy** [ [config save required](#) ]
 Logged in as: **admin** [ [logout](#) ]

- Optimization Service
- Host Settings
- **Advanced Networking**
  - Asymmetric Routing
  - Connection Forwarding
  - **Encryption** «
  - Failover Settings
  - NetFlow
  - Peering Rules
  - QoS Classification
  - QoS Marking
  - Service Ports
  - Simplified Routing
  - WCCP Groups
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

[Configuration Manager](#) (1)

- Upgrade Software
- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

### Advanced Networking - Encryption

The encryption feature allows data to be communicated securely with other appliances.

**General**

☐ Enable Authentication and Encryption
 ☒ Enable Perfect Forward Secrecy

Encryption Policy:
 Method 1: DES
Method 2: None

Authentication Policy:
 Method 1: MD5
Method 2: None

Time Between Key Renegotiations: 240 (minutes)

Enter the Shared Secret:

Confirm the Shared Secret:

[Apply](#)

Peer	Encryption	Authentication	State	Duplex	Time Created
No secure connections with peer appliances.					

[Remove Selected Entries](#)

**Add New Peer:**

Peer IP:

[Add Peer](#)

[Save](#)
[Reset](#)

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p>Check one or more of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Enable Authentication and Encryption.</b> Specify this option to enable authentication between appliances.</li> <li>• <b>Enable Perfect Forward Secrecy.</b> Specify this option if you want to provide additional security by renegotiating keys at specified intervals. Perfect Forward Secrecy provides additional security by renegotiating keys at specified intervals. If one key is compromised, subsequent keys are secure because they are not derived from previous keys.</li> </ul> <hr/> <p><b>Encryption Policy.</b> Select one of the following methods from the <b>Method 1</b> drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>DES.</b> Data Encryption Standard. <b>DES</b> is the default value.</li> <li>• <b>NULL.</b> Specifies the null encryption algorithm.</li> </ul> <p>Set encryption algorithms in order of priority. The algorithm is used to encrypt each packet sent using IPsec.</p> <p>Optionally, select <b>DES</b>, <b>NULL</b>, or <b>None</b> from the <b>Method 2</b> drop-down list.</p> <hr/> <p><b>Authentication Policy.</b> Select one of the following authentication methods from the <b>Method One</b> drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>MD5.</b> Message-Digest algorithm. <b>MD5</b> is a widely-used cryptographic hash function with a 128-bit hash value. <b>MD5</b> is the default value.</li> <li>• <b>SHA-1.</b> Secure Hash Algorithm. <b>SHA-1</b> is a set of related cryptographic hash functions. <b>SHA-1</b> is considered to be the successor to <b>MD5</b>.</li> </ul> <p>Optionally, select <b>MD5</b>, <b>SHA-1</b>, or <b>None</b> from the <b>Method Two</b> drop-down list.</p> <hr/> <p><b>Time Between Key Renegotiations.</b> Specify the number of minutes between quick-mode renegotiation of keys using Internet Key Exchange (IKE). IKE uses public key cryptography to provide the secure transmission of a secret key to a recipient so that the encrypted data can be decrypted at the other end. The default value is <b>240</b> minutes.</p> <hr/> <p><b>Enter the Shared Secret/Confirm the Shared Secret.</b> Specify the shared secret. All the HP EFS WAN Accelerators in a network for which you want to use IPsec must have the same shared secret.</p> <hr/> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.</p>
Add New Peer	<p><b>Peer IP.</b> Specify the IP address for the peer HP EFS WAN Accelerator for which you want to make a secure connection.</p> <hr/> <p><b>Add Peer.</b> Click <b>Add Peer</b> to add the peer specified in the <b>Peer IP</b> text box.</p> <p>If IPsec is enabled on this HP EFS WAN Accelerator, then it must also be enabled on all appliances in the IP security peers list; otherwise this HP EFS WAN Accelerator will not be able to make optimized connections with those peers.</p> <p>If a connection has not been established between the two HP EFS WAN Accelerators that are configured to use IPsec security, the Peers list does not display the peer HP EFS WAN Accelerator because a security association has not been established.</p> <hr/> <p><b>Remove Selected Peers.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Peers</b>.</p>

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.



## Enabling Failover and Data Store Synchronization

You enable failover and automatic data store synchronization support in the Advanced Networking - Failover Settings page.

Failover support ensures continued optimization if there is a failure with one of the HP EFS WAN Accelerators. If the master HP EFS WAN Accelerator fails, the traffic is automatically processed by the backup HP EFS WAN Accelerator.

Automatic data store synchronization replicates the data store from an *active* HP EFS WAN Accelerator to a *passive* HP EFS WAN Accelerator without disrupting operations. Data store synchronization ensures that a *warm* data store exists on the backup HP EFS WAN Accelerator. With a warm data store, the backup HP EFS WAN Accelerator can perform as optimally as its master when it is activated; that is, it performs as if it has seen the data before and only sends new segments across the WAN.

---

**NOTE:** Data is replicated only from the master HP EFS WAN Accelerator to the backup; not vice versa.

---



---

**NOTE:** All operations occur in the background and do not disrupt operations on any of the systems.

---

Enable data store synchronization if you have:

- ◆ **Simple Redundancy.** A network in which two HP EFS WAN Accelerators have been deployed in a failover configuration.
- ◆ **Router Redundancy.** A network where there two or more routers at a remote site and HP EFS WAN Accelerators are deployed behind each router for redundancy.
- ◆ **Complex Router Redundancy.** A network where serially connected HP EFS WAN Accelerators containing multi-port cards that connect to multiple routers on each side of the network.
- ◆ **Virtual In-Path and Out-of-Path.** An out-of-path deployment or a virtual in-path deployment using WCCP, PBR, or a Layer-4 switch.
- ◆ **Serial Cluster.** A network where several HP EFS WAN Accelerators are deployed back-to-back in an in-path configuration.

Enabling failover and data synchronization support is *optional*.

## To enable failover and data store synchronization

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click Failover Settings to display the Advanced Networking - Failover Settings page.

Figure 2-28. Advanced Networking - Failover Settings Page

The screenshot displays the 'Advanced Networking - Failover Settings' page. At the top, there is a navigation bar with links: Home, Setup, Reports, Logging, and Help. The 'Setup' link is highlighted. To the right of the navigation bar, the status is 'Healthy' and the user is logged in as 'admin'. On the left side, there is a sidebar menu with various configuration options. The 'Advanced Networking' menu is expanded, and 'Failover Settings' is selected. The main content area is titled 'Advanced Networking - Failover Settings' and contains a sub-header 'Configure your appliance failover configuration.' Below this, there are two sections: 'Failover Settings' and 'Automated Online Data Store Synchronization Settings'. The 'Failover Settings' section has a checkbox for 'Enable Failover Support' which is currently unchecked. Below this checkbox, there are two fields: 'Current Appliance is the:' with a dropdown menu set to 'Master', and 'Other Appliance's Inpath IP Address:' with an empty text input field. The 'Automated Online Data Store Synchronization Settings' section also has a checkbox for 'Enable Automated Online Data Store Synchronization' which is unchecked. Below this checkbox, there are four fields: 'Current Appliance is the:' with a dropdown menu set to 'Backup', 'Other Appliance's IP Address:' with an empty text input field and a note '(via Primary or AUX interfaces)', 'Synchronization Port:' with a text input field containing '7744', and 'Reconnection interval:' with a text input field containing '30' and the unit 'secs'. At the bottom right of the page, there are two buttons: 'Apply' and 'Save'.

Home : Setup : Reports : Logging : Help Status: **Healthy** Logged in as: admin

### Advanced Networking - Failover Settings

Configure your appliance failover configuration.

#### Failover Settings

☐ Enable Failover Support

Current Appliance is the: Master

Other Appliance's Inpath IP Address:

#### Automated Online Data Store Synchronization Settings

☐ Enable Automated Online Data Store Synchronization

Current Appliance is the: Backup

Other Appliance's IP Address:  (via Primary or AUX interfaces)

Synchronization Port:

Reconnection interval:  secs

Apply Save

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Failover Settings	<p><b>Enable Failover Support.</b> Specify this option to enable failover support.</p> <hr/> <p><b>Current Appliance is the.</b> Select <b>Master</b> or <b>Backup</b> from the drop-down list. A master HP EFS WAN Accelerator is the primary appliance; the backup HP EFS WAN Accelerator is the appliance that automatically optimizes traffic if the master appliance fails. You must specify the primary IP address for the backup appliance.</p> <p><b>IMPORTANT:</b> If you have multiple bypass cards installed in your appliance you must specify the <b>inpath0_0</b> interface for the in-path IP address.</p> <p><b>NOTE:</b> If you have an out-of-path configuration with failover support, you must specify the master and backup appliances in the Optimization Service - In-Path Rules page. For detailed information, see <a href="#">“Setting In-Path Rules” on page 25</a>.</p> <hr/> <p><b>Other Appliance’s In-path IP Address.</b> Specify the IP address for the master or backup HP EFS WAN Accelerator. You must specify the in-path IP address (<b>inpath0_0</b>) for the HP EFS WAN Accelerator, not the primary interface IP address.</p> <p><b>IMPORTANT:</b> If you have multiple bypass cards installed in your HP EFS WAN Accelerator you must specify the <b>inpath0_0</b> interface for the in-path IP address.</p> <p>For detailed information, see <a href="#">“Setting In-Path Interfaces” on page 54</a>.</p>

Control	Description
Automated Online Datastore Settings	<p><b>Enable Automated Online Datastore Synchronization.</b> Specify this option to enable automated data store synchronization. Data store synchronization ensures that each data store in your network has warm data for maximum optimization. All operations occur in the background and do not disrupt operations on any of the systems.</p> <p>There are the following phases in synchronization:</p> <ul style="list-style-type: none"> <li>• <b>Catchup.</b> Copies data that is already on the master to the backup HP EFS WAN Accelerator. This process stops when all the old data from the master is copied to the backup HP EFS WAN Accelerator.</li> <li>• <b>Keepup.</b> Runs continuously copying new data that the master appliance encounters to the backup HP EFS WAN Accelerator.</li> </ul> <p><b>IMPORTANT:</b> The HP EFS WAN Accelerators must be the same model; models running different versions of the software will not synchronize (for example v2.x to 3.x). Synchronization does not guarantee that all data objects are replicated—synchronization runs in the background, if the HP EFS WAN Accelerator is under load, all data may not be replicated.</p> <p><b>NOTE:</b> If you are setting up automated data store synchronization for the first time, the HP EFS WAN Accelerator service is halted on the backup HP EFS WAN Accelerator. You must restart the HP EFS WAN Accelerator service on backup HP EFS WAN Accelerators. If you restart the service with a clean data store you must shutdown the backup HP EFS WAN Accelerator, power it off, and power it on.</p> <p><b>NOTE:</b> In out-of-path configurations, you must designate an HP EFS WAN Accelerator as a backup appliance, either by enabling failover support or by designating it as an out-of-path backup appliance, to implement data store synchronization.</p> <hr/> <p><b>Current Appliance is the.</b> Select <b>Master</b> or <b>Backup</b> from the drop-down list. You must specify the primary IP address for the master and backup appliance.</p> <p><b>IMPORTANT:</b> If you have multiple bypass cards installed in your appliance you must specify the <b>inpath0_0</b> interface.</p> <hr/> <p><b>Other Appliance's In-path IP Address.</b> Specify the backup or master HP EFS WAN Accelerator IP address. You must specify the primary IP address for the master and backup appliance.</p> <p>You must specify the primary (or AUX if you have enabled this option) IP address for the HP EFS WAN Accelerator. For detailed information, see <a href="#">“Setting the Primary Interface” on page 52</a>.</p> <p><b>IMPORTANT:</b> If you have multiple bypass cards installed in your appliance you must specify the <b>inpath0_0</b> interface.</p> <hr/> <p><b>Synchronization Port.</b> Specify the port number for the HP EFS WAN Accelerator from which you want to replicate data. The default value is <b>7744</b>.</p> <hr/> <p><b>Reconnection interval.</b> Specify the number of seconds. The default value is <b>30</b>.</p>

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

---

**NOTE:** If you are setting up automated data store synchronization for the first time, you must restart the HP EFS WAN Accelerator service on both the master and the backup HP EFS WAN Accelerators to initialize data store synchronization. For detailed information about restarting the HP EFS WAN Accelerator service, see the [“Starting and Stopping Services” on page 144](#).

---

---

**NOTE:** In an out-of-path configuration, to implement failover support, you must also specify a fixed target rule that specifies both master and backup target appliances. For detailed information, see [“Setting In-Path Rules” on page 25](#).

---

## Enabling NetFlow

You enable and configure NetFlow support in the Advanced Networking - NetFlow Export page.

NetFlow enables you to export network statistics that provide information about network users and applications, peak usage times, and traffic routing. NetFlow records information for each packet ingressing the specified network interface. This data is then sent to a NetFlow collector, a software package provided by a third party vendor or an open source.

---

**IMPORTANT:** Enabling NetFlow could adversely impact HP EFS WAN Accelerator performance and increase bandwidth utilization.

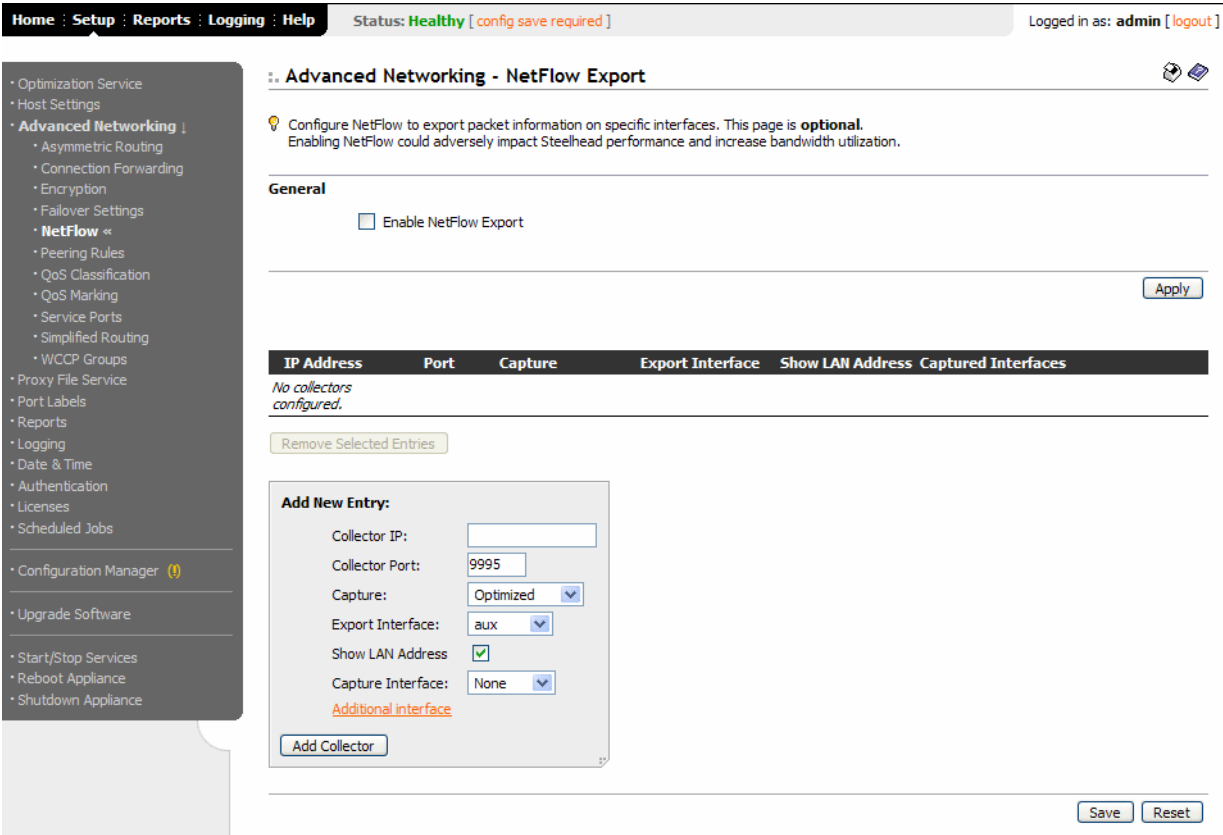
---

Enabling NetFlow support is *optional*.

**To enable NetFlow support**

- 1. Click the Setup tab to display the Setup menu.
- 2. Click Advanced Networking to expand the Advanced Networking menu.
- 3. Click NetFlow to display the Advanced Networking - NetFlow Export page.

**Figure 2-29.** Advanced Networking - NetFlow Export Page



- 4. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<b>Enable NetFlow Export.</b> Specify this option to enable NetFlow support.
	<b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.

Control	Description
Add New Entry	<p><b>Collector IP.</b> Specify the IP address for the NetFlow collector.</p> <p><b>Collector Port.</b> Specify the port the NetFlow collector is listening on. The default value is <b>2055</b>.</p> <p><b>Capture.</b> Select <b>Optimized</b>, <b>Passthrough</b>, or <b>All</b> from the drop-down list. Specifies whether optimized, pass through, or all traffic is exported to the NetFlow collector. The default value is <b>Optimized</b>.</p> <p><b>Export Interface.</b> Select <b>aux</b> or <b>primary</b> from the drop-down list. NetFlow records sent from the HP EFS WAN Accelerator will appear to be sent from the IP address of the selected interface.</p> <p><b>Show LAN Address.</b> Specify this option if the TCP IP addresses and ports reported for optimized flows should contain the original client and server IP addresses and not those of the HP EFS WAN Accelerator. The default is to show the IP addresses of the original client and server without the IP address of the HP EFS WAN Accelerators.</p> <p><b>Capture Interface.</b> Select from the drop-down list the interface on which NetFlow should track flows.</p> <p><b>Additional Interface.</b> Click the <b>Additional interface</b> to display an additional <b>Capture Interface</b> drop-down list.</p> <p><b>Add Collector.</b> Click <b>Add Collector</b> to add the collector to the Collector list.</p> <p><b>Remove Selected Entries.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Peers</b>.</p>

## Setting Peering Rules

You set peering relationships among HP EFS WAN Accelerators in the Advanced Networking - Peering Rules page. Serial clusters are supported only on Series 5000s.

You can configure peering rules that apply to a single port or you can configure peering rules that apply to a *port label*. A port label is a label that you assign to a set of ports so that you can reduce the number of configuration rules in your system. For detailed information about how to configure port labels, see [“Creating Port Labels” on page 113](#).

## Enabling Peering Rules for Serial Clustering

You can provide increased optimization by deploying several HP EFS WAN Accelerators back-to-back in an in-path configuration to create a serial cluster. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

Appliances in a cluster process the peering rules you specify in a *spill-over* fashion. When the maximum number of TCP connections for an HP EFS WAN Accelerator is reached, that appliance stops intercepting new connections and passes them on to the next HP EFS WAN Accelerator in the cluster (as defined by the peer rule that you set).

In serial cluster deployments:

- ◆ The peering rules table is a ordered list of rules and the first rule that matches the rule is applied.
- ◆ To avoid interceptions on inner connections created by other appliances in the same cluster, in-path rules are specified to pass-through connections originating from those appliances.

Setting peering rules to enable serial clustering is *optional*.

---

**IMPORTANT:** HP strongly recommends that only Series 5000s are deployed in a serial cluster due to traffic loads.

---

For detailed information about serial cluster deployments and peering rules, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

## To set a peering rule

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click Peering Rules to display the Advanced Networking - Peering Rules page.

**Figure 2-30.** Advanced Networking - Peering Rules Page

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: **admin** [ logout ]

**Advanced Networking - Peering Rules**

The peering rules feature allows you to define appliance peering relationships. Note that only the first matching rule will be applied.

#	Type	Source	Destination	Port	Peer
def	Auto	All	All	All	All

Remove Selected Rules

**Add New Rule:**

Type:     Insert Rule At:

Source Subnet:     Destination Subnet:     Port:

Peer IP:

Description:

Add Rule

Save    Reset



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Rule	<p><b>Type.</b> Select one of the following rule types from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Auto.</b> Allows built-in functionality to determine the response for peering requests (performs the best peering possible).</li> <li>• <b>Accept.</b> Accepts peering requests that match the source-destination-port pattern.</li> <li>• <b>Pass.</b> Allows pass-through peering requests that match the source and destination port pattern.</li> </ul> <p>You can configure peering rules that apply to a single port or you can configure peering rules that apply to a port label. A port label is a label that you assign to a set of ports so that you can reduce the number of configuration rules in your system. For detailed information about how to configure port labels, see <a href="#">“Creating Port Labels” on page 113</a>.</p> <hr/> <p><b>Insert Rule At.</b> Select <b>start</b>, <b>end</b>, or a rule number from the drop-down list.</p> <p>HP EFS WAN Accelerators evaluate rules in numerical order starting with rule <b>1</b>. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule <b>1</b> do not match, rule <b>2</b> is consulted. If rule <b>2</b> matches the conditions, it is applied, and no further rules are consulted.</p> <hr/> <p><b>Source Subnet.</b> Specify the IP address for the source network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <hr/> <p><b>Destination Subnet.</b> Specify the IP address for the destination subnet. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <hr/> <p><b>Port.</b> Specify the destination port number, port label, or <b>all</b>. For detailed information on port labels, see <a href="#">“Creating Port Labels” on page 113</a>.</p> <hr/> <p><b>Peer IP.</b> Specify the IP address for the peer to which TCP requests should spill over when the HP EFS WAN Accelerator reaches its built-in capacity limit.</p> <hr/> <p><b>Description.</b> Specify a description to help you identify the peering relationship.</p> <hr/> <p><b>Add Rule.</b> Specify this option to add the rule to the list of rules for the profile.</p> <hr/> <p><b>Remove Selected Rules.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Rules</b>.</p> <hr/> <p><b>Move Rule.</b> Use the <b>Move Rule</b> drop-down list boxes and button to change the order in which rules are evaluated.</p>

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling Quality of Service

You enable Quality of Service (QoS) in the Advanced Networking - QoS Classification page.

You can configure QoS on HP EFS WAN Accelerators to control the prioritization of different types of network traffic and to ensure that HP EFS WAN Accelerators give certain network traffic (for instance, voice over IP) higher priority than other network traffic.

QoS allows you to specify priorities for various classes of traffic and properly distributes excess bandwidth among classes. The HP EFS WAN Accelerator allows you to decouple priority (in terms of delay) from the bandwidth allocation. This provides the flexibility needed to support varying degrees of priority and bandwidth traffic patterns, such as high-priority, low-bandwidth traffic patterns (for example, Telnet). Many QoS schemes use the term priority to specify how to control the excessive bandwidth among different classes. In the HP EFS WAN Accelerator, priority actually refers to traffic *delays* and excessive bandwidth is shared, proportional to the minimum bandwidth guaranteed for a specific class.

Enabling this feature is *optional*.

**To enable QoS classification**

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click QoS Classification to display the Advanced Networking - QoS Classification page.

Figure 2-31. Advanced Networking - QoS Classification Page

Home

Setup

Reports

Logging

Help

Status: Healthy [ config save required ]

Logged in as: admin [ logout ]

Optimization Service

Host Settings

Advanced Networking

Asymmetric Routing

Connection Forwarding

Encryption

Fallover Settings

NetFlow

Peering Rules

QoS Classification

QoS Marking

Service Ports

Simplified Routing

WCCP Groups

Proxy File Service

Port Labels

Reports

Logging

Date & Time

Authentication

Licenses

Scheduled Jobs

Configuration Manager

Upgrade Software

Start/Stop Services

Reboot Appliance

Shutdown Appliance

Advanced Networking - QoS Classification

The QoS classification feature allows you to prioritize both optimized and passthrough traffic going through this appliance.

General

Enable QoS Classification

WAN Bandwidth for Interface **wan0\_0**:  kbps

Apply

Configure your QoS classes.

Click on the name of a class to edit its details.

QoS Class	Priority	Guaranteed BW%
default	Normal Priority	0.01
<input type="checkbox"/> tere	Real-Time	56.00
<input type="checkbox"/> test	Real-Time	5.00
<input type="checkbox"/> tjekrl	Business Critical	33.00

Remove Selected Classes

Add New QoS Class:

Class Name:

Priority:

Guaranteed BW:  %

Add QoS Class

Configure your QoS rules.

Note that only the first matching rule will be applied.

#	Class Name	Source	Destination	Protocol	DSCP	VLAN	Type
<input type="checkbox"/> 1	default	All:All	All:All	TCP	All	All	All
<input type="checkbox"/> 2	default	All:3	All:All	TCP	All	All	All
	def default	All:All	All:All	All	All	All	All

Remove Selected Rules

Move Rule:  to

Move Rule

Add New Rule:

Insert Rule At:

Class Name:

Source Subnet:  Port:

Destination Subnet:  Port:

Protocol:

Traffic Type:

DSCP:  (optional)

VLAN:  (optional)

Add Rule

Save Reset

2 CONFIGURING THE HP EFS  
WAN ACCELERATOR

HP STORAGEWORKS EFS WAN ACCELERATOR MANAGEMENT CONSOLE USER GUIDE

83

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p><b>Enable QoS Classification.</b> Specify this option to enable QoS.</p> <hr/> <p><b>WAN Bandwidth for Interface XXXX-X.</b> Specify the bandwidth link rate for the WAN interface.</p> <p>This is the <i>bottleneck</i> WAN bandwidth not the interface speed out of the WAN interface into the router or switch. For example, if your HP EFS WAN Accelerator connects to a router with a 100 Mbps link, do not specify this value—specify the actual WAN bandwidth (for example, T1, T3).</p> <p><b>IMPORTANT:</b> Different WAN interfaces can have different WAN bandwidths; this value must be correctly entered for QoS to function correctly.</p> <p><b>IMPORTANT:</b> The percentage of excess bandwidth give to a class is relative to the percentage of minimum bandwidth allocated to the class.</p> <hr/> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.</p>
Add New QoS Class	<p><b>Class Name.</b> Specify a name for the QoS class.</p> <p><b>TIP:</b> You must enable QoS classification and set the bandwidth link rate for the WAN interface to create a QoS class.</p> <hr/> <p><b>Priority.</b> Select a priority type from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Real-Time.</b> Specifies real-time traffic class. Traffic that is your highest priority should be given this value.</li> <li>• <b>Interactive.</b> Specifies an interactive traffic class.</li> <li>• <b>Business Critical.</b> Specifies the business critical traffic class.</li> <li>• <b>Normal Priority.</b> Specifies normal priority traffic class.</li> <li>• <b>Low Priority.</b> Specifies low priority traffic class. Traffic that is your lowest priority should be given this value.</li> </ul> <p>Priorities are listed in decreasing order of importance. These are minimum priority guarantees, if better service is available it is provided. For example, if a class is specified as <b>Low Priority</b> and the higher priority classes are not active, then the <b>Low Priority</b> class is given the highest possible priority for the current traffic conditions.</p> <hr/> <p><b>Guaranteed BW.</b> Specify the bandwidth amount that you want to guarantee for a specific class. All the classes combined cannot exceed 100%. During contention for bandwidth the class is guaranteed for the amount specified, it will receive more bandwidth if there is unused bandwidth remaining.</p> <p><b>NOTE:</b> The percentage of excess bandwidth given to a class is relative to the percentage of the minimum bandwidth allocated in the WAN Bandwidth for Interface field.</p> <hr/> <p><b>Add QoS Class.</b> Click <b>Add QoS Class</b> to add a class to the QoS class list.</p> <hr/> <p><b>Remove Selected Classes.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Classes</b>.</p>

Control	Description
Add New Rule	<p><b>Insert Rule At.</b> To create a QoS rule for a QoS class, select <b>start</b>, <b>end</b>, or a rule number from the drop-down list. Specify an ordered list of rules.</p> <p>HP EFS WAN Accelerators evaluate rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.</p> <hr/> <p><b>Class Name.</b> Select a class name from the drop-down list. If the rule matches, the specified rule sends the packet to this class.</p> <hr/> <p><b>Source Subnet.</b> Specify the IP address for the source network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <p><b>Port.</b> Specify the port for the source subnet. The default value is <b>All</b>.</p> <hr/> <p><b>Destination Subnet.</b> Specify the IP address for the destination network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <p><b>Port.</b> Specify the port for the destination port. The default value is <b>All</b>.</p> <hr/> <p><b>Protocol.</b> Select <b>All</b>, <b>TCP</b>, or <b>UDP</b> from the drop-down list.</p> <hr/> <p><b>Traffic Type.</b> Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Real-Time.</b> Specifies real-time traffic class. Traffic that is your highest priority should be given this value.</li> <li>• <b>Interactive.</b> Specifies an interactive traffic class.</li> <li>• <b>Business Critical.</b> Specifies the business critical traffic class.</li> <li>• <b>Normal Priority.</b> Specifies normal priority traffic class.</li> <li>• <b>Low Priority.</b> Specifies low priority traffic class. Traffic that is your lowest priority should be given this value.</li> </ul> <hr/> <p><b>DSCP.</b> Optionally, specify the DSCP level.</p> <hr/> <p><b>VLAN.</b> Optionally, specify the VLAN tag for the rule.</p> <hr/> <p><b>Add Rule.</b> Click <b>Add Rule</b> to add a rule to the QoS rule list.</p> <hr/> <p><b>Remove Selected Rules.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Rules</b>.</p> <hr/> <p><b>Move Rule.</b> Select a rule to move and the position where you want to move it to. Click <b>Move Rule</b> to apply your changes.</p>

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying a QoS Class

You can modify a QoS class in the Advanced Networking - QoS Classification <class name> page.

## To modify a QoS class

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click QoS Classification to display the Advanced Networking - QoS Classification page.
4. Click the class name in the Classification List to display the Advanced Networking - QoS Classification page

**Figure 2-32. Advanced Networking - QoS Classification Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ] [ restart required ]    Logged in as: admin [ logout ]

---

- Optimization Service
- Host Settings
- **Advanced Networking** ↓
  - Asymmetric Routing
  - Connection Forwarding
  - Encryption
  - Failover Settings
  - NetFlow
  - Peering Rules
  - **QoS Classification** «
  - QoS Marking
  - Service Ports
  - Simplified Routing
  - WCCP Groups
- Proxy File Service
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

---

- Configuration Manager ( ! )

---

- Upgrade Software

---

- Start/Stop Services ( ! )
- Reboot Appliance
- Shutdown Appliance

### Advanced Networking - QoS Classification

💡 Update your QoS class.

---

**QoS Class: test**

Priority:

Guaranteed BW:  %

Upper BW:  % *(optional)*

---

5. Use the controls to complete the configuration, as described in the following table.

Control	Description
QoS Class	<p><b>Priority.</b> Select a priority type from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Real-Time.</b> Specifies real-time traffic class. Traffic that is your highest priority should be given this value.</li> <li>• <b>Interactive.</b> Specifies an interactive traffic class.</li> <li>• <b>Business Critical.</b> Specifies the business critical traffic class.</li> <li>• <b>Normal Priority.</b> Specifies normal priority traffic class.</li> <li>• <b>Low Priority.</b> Specifies low priority traffic class. Traffic that is your lowest priority should be given this value.</li> </ul> <hr/> <p><b>Guaranteed BW.</b> Specify the bandwidth amount that you want to guarantee for a specific class. All the classes combined cannot exceed 100%. During contention for bandwidth the class is guaranteed for the amount specified, it will receive more bandwidth if there is unused bandwidth remaining.</p> <p><b>NOTE:</b> The percentage of excess bandwidth given to a class is relative to the percentage of the minimum bandwidth allocated in the WAN Bandwidth for Interface field.</p> <hr/> <p><b>Upper BW.</b> Optionally, specify the upper bandwidth limit. Specifies the maximum amount (percentage) of allowed bandwidth a flow will receive regardless of excess bandwidth available.</p>

6. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
7. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting QoS Marking

You set QoS marking in the Advanced Networking - QoS Marking page.

The QoS feature allows you to enforce a DSCP level for optimized connections. The DSCP level corresponds to the DiffServ DSCP field in the IP packets header. After you map a source-destination-port pattern and a DSCP level, every packet corresponding to the connection with that destination port has the DSCP field set to that value in the forward and backward direction. On the WAN side of the HP EFS WAN Accelerator, you configure a network router or a traffic shaper to prioritize packets according to the value in the DSCP field before they are sent across the WAN.

After you map a destination port and a DSCP level, every packet corresponding to the connection with that destination port has the DSCP field set to that value in the forward and backward direction. On the WAN side of the HP EFS WAN Accelerator, you configure a network router or a traffic shaper to prioritize packets according to the value in the DSCP field before they are sent across the WAN.

Note that only the first matching mapping will be applied.

Enabling this feature is *optional*.

## To set a QoS marking

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click QoS Rules to display the Advanced Networking - QoS Marking page.

**Figure 2-33. Advanced Networking - QoS Marking Page**

The screenshot shows the 'Advanced Networking - QoS Marking' page. At the top, there is a navigation bar with 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The 'Setup' tab is active. Below the navigation bar, the status is 'Healthy [config save required]' and the user is logged in as 'admin [logout]'. On the left, a sidebar menu lists various configuration options, with 'QoS Marking' selected. The main content area has a title 'Advanced Networking - QoS Marking' and a note: 'The QoS marking feature allows you to map a service port to a Differentiated Services CodePoint. Note that only the first matching mapping will be applied.' Below this is a table with columns '#', 'Source', 'Destination', 'Port', and 'DSCP'. The table contains one row: 'def All', 'All', 'All', 'Reflect'. Below the table is a button 'Remove Selected Mappings'. Below that is a form titled 'Add New Mapping:' with fields for 'Insert Rule At:' (dropdown set to 'end'), 'Source Subnet:' (text box 'all'), 'Destination Subnet:' (text box 'all'), 'Port:' (text box 'all'), 'DSCP:' (dropdown set to 'reflect'), and 'Description:' (text box). There is an 'Add Mapping' button at the bottom of the form. At the bottom right of the page are 'Save' and 'Reset' buttons.

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: **admin** [ logout ]

**Advanced Networking - QoS Marking**

The QoS marking feature allows you to map a service port to a Differentiated Services CodePoint.  
Note that only the first matching mapping will be applied.

#	Source	Destination	Port	DSCP
def	All	All	All	Reflect

Remove Selected Mappings

**Add New Mapping:**

Insert Rule At: end  
Source Subnet: all    Destination Subnet: all    Port: all  
DSCP: reflect  
Description:

Add Mapping

Save    Reset



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Mappings	<p><b>Insert Rule At.</b> Select <b>start</b>, <b>end</b>, or a rule number from the drop-down list. Specify an ordered list of rules where each rule is the DSCP level used on the inner connection for connections matching the source IP subnet, the destination IP subnet and, optionally, the destination port fields.</p> <p>HP EFS WAN Accelerators evaluate rules in numerical order starting with rule <b>1</b>. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule <b>1</b> do not match, rule <b>2</b> is consulted. If rule <b>2</b> matches the conditions, it is applied, and no further rules are consulted.</p> <p><b>Source Subnet.</b> Specify the IP address for the source network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <p><b>Destination Subnet.</b> Specify the IP address for the destination network. Use the following format: <b>XXX.XXX.XXX.XXX/XX</b>.</p> <p><b>Port.</b> Specify the port number or port label. A port label is a label that you assign to a set of ports so that you can reduce the number of configuration rules in your system. For detailed information about how to configure port labels, see <a href="#">“Creating Port Labels” on page 113</a>.</p> <p>For the MAPI data channel, specify port <b>7830</b> and the corresponding DSCP level.</p> <p>For the FTP data channel, specify port <b>20</b> and the corresponding DSCP level. Setting QoS for port <b>20</b> on the client-side HP EFS WAN Accelerator effects passive FTP, while setting the QoS for port <b>20</b> on the server-side HP EFS WAN Accelerator effects port active FTP.</p> <p><b>DSCP.</b> Specify the DSCP level (<b>0-63</b>). Specify a DSCP level to use instead of the existing DSCP level. If you do not define a DSCP level, the HP EFS WAN Accelerator uses the existing DSCP level.</p> <p><b>IMPORTANT:</b> If your connections already have a DSCP level and you do not define one in the Management Console, the HP EFS WAN Accelerator uses the existing DSCP level for the connection between the HP EFS WAN Accelerators. If you define a DSCP level in the Management Console, the HP EFS WAN Accelerator overrides the existing DSCP level and the value that you defined is applied.</p> <p><b>Description.</b> Specify a description of the QoS rule.</p> <p><b>Add Rule.</b> Click <b>Add Rule</b> to add a rule to the QoS rule list.</p> <p><b>Remove Selected Rules.</b> To remove an entry, click the check box next to the name and click <b>Remove Selected Rules</b>.</p>

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying QoS Marking Descriptions

You can modify the description of your QoS marking rules in the Advanced Networking - QoS Marking Edit page.

## To modify your QoS rule description

1. Click the Setup tab to expand the Optimization Service menu.
2. Click Advanced Networking expand the Advanced Networking menu.
3. Click Qos Marking to display the Advanced Networking - QoS Marking page.
4. Click **Edit Desc** in the QoS Rules table to display the Optimization Service - In-Path Rules Edit page.

**Figure 2-34.** Advanced Networking - QoS Marking Edit Page

The screenshot shows the 'Advanced Networking - QoS Marking' edit page. On the left is a sidebar with a tree view containing items like 'Optimization Service', 'Host Settings', 'Advanced Networking', 'QoS Marking', and others. The top navigation bar includes 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status bar shows 'Status: Healthy' and 'Logged in as: admin [logout]'. The main content area is titled 'Advanced Networking - QoS Marking' and contains a message 'Update your QoS rule.' Below this is a 'Description' section with a text input field containing 'mmichon - test'. There are 'Update Description' and 'Cancel' buttons. At the bottom right of the main area are 'Save' and 'Reset' buttons.

5. Modify the description of the QoS rule in the text box and click **Update Description**.
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying Service Ports

You can modify service port settings in the Advanced Networking - Service Ports page.

Service ports are the ports used for inner connections between HP EFS WAN Accelerators.

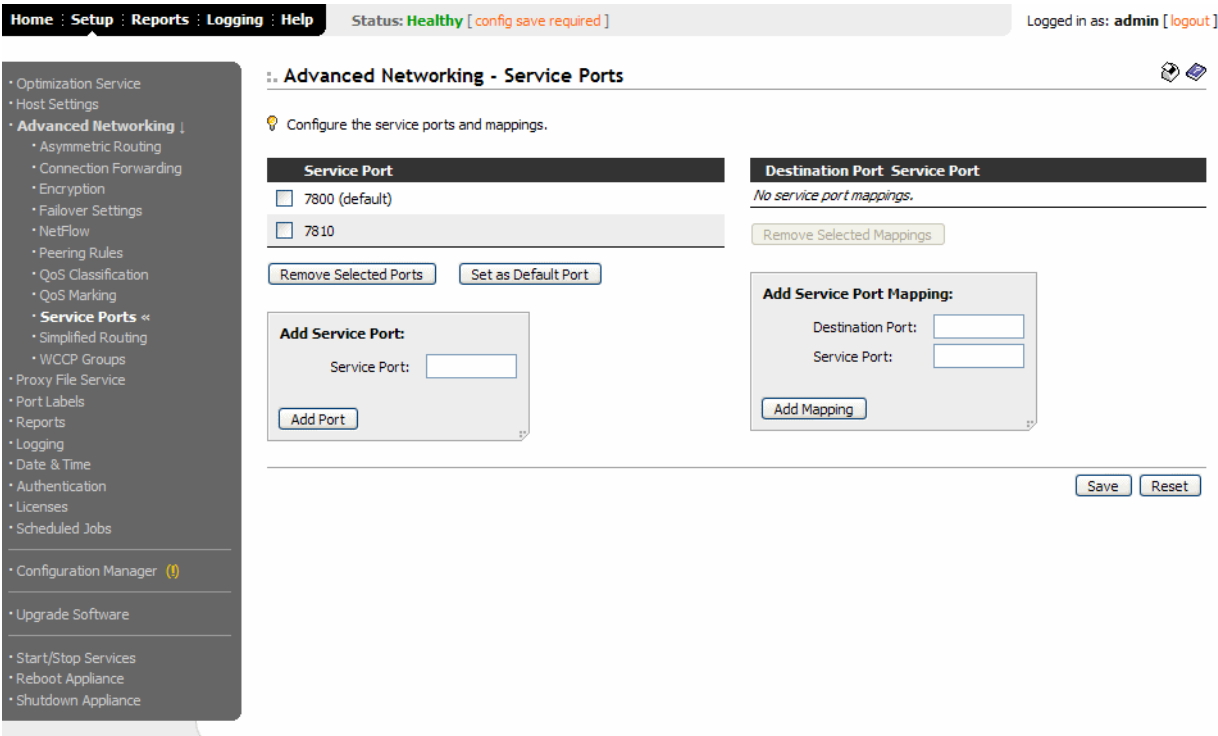
You can configure multiple service ports on the server-side of the network for multiple QoS mappings. You define a new service port and then map destination ports to that port, so that QoS configuration settings on the router are applied to that service port.

Modifying service port settings is *optional*.

To set a service port

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click Service Ports to display the Advanced Networking - Service Ports page.

Figure 2-35. Advanced Networking - Service Ports Page



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add Service Port	<b>Service Port.</b> Specify a port number. The default service ports are <b>7800</b> and <b>7810</b> .
	<b>Add Port.</b> Click <b>Add Port</b> to add the port to the service port list.
	<b>Set As Default Port.</b> To set a port as the default port, select it and click <b>Set As Default Port</b> .
	<b>Remove Selected Port.</b> To remove an entry, select it and click <b>Remove Selected Port</b> .
Add Service Port Mapping	<b>Destination Port.</b> Specify a destination port number.
	<b>Service Port.</b> Specify a port number.
	<b>Add Mapping.</b> Click <b>Add Mapping</b> to add a mapping to the mappings list.
	<b>Remove Selected Mappings.</b> To remove an entry, select it and click <b>Remove Selected Mappings</b> .

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling Simplified Routing

You can enable simplified routing in the Advanced Networking - Simplified Routing page.

Simplified routing collects the IP address for the next hop Media Access Control (MAC) address from each packet it receives to use in addressing traffic. Enabling simplified routing eliminates the need to add static routes when the HP EFS WAN Accelerator is in a different subnet from the client and server.

Without simplified routing if an HP EFS WAN Accelerator is installed in a different subnet from the client or server, you must define one router as the default gateway and static routes for the other routers so that traffic is not redirected back through the HP EFS WAN Accelerator. In some cases, even with the static routes defined, the Access Control List (ACL) on the default gateway may still drop traffic that should have gone through the other router.

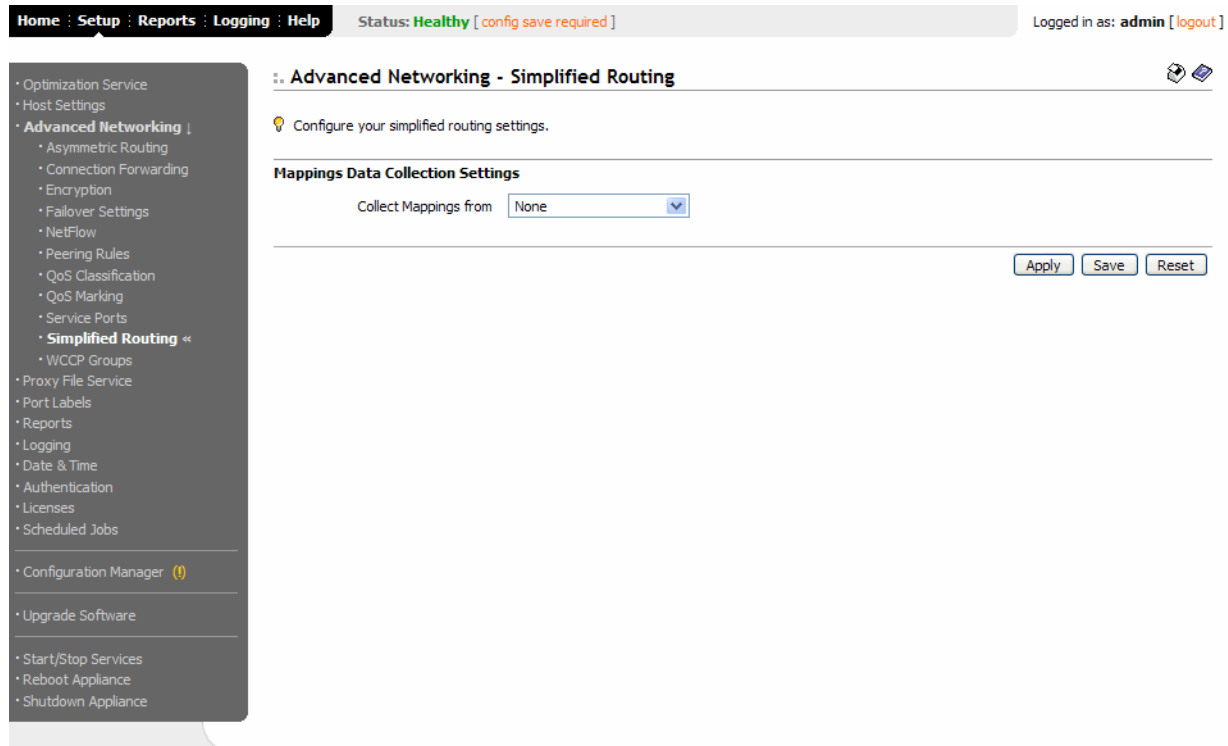
Simplified routing has the following constraints:

- ◆ Broadcast support in Proxy File Service configurations cannot be enabled.
- ◆ WCCP cannot be enabled.
- ◆ Connection forwarding cannot be enabled if you collect mappings for source MAC data (that is, the options **all** or **dest-source**).
- ◆ The default route must exist on each HP EFS WAN Accelerator in your network.
- ◆ Simplified routing requires a client-side and server-side HP EFS WAN Accelerator.

## To enable simplified routing

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click Simplified Routing to display the Advanced Networking - Simplified Routing page.

Figure 2-36. Advanced Networking - Simplified Routing Page



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Mappings Data Collection Settings	<p><b>Collect Mappings from.</b> Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>None.</b> All options are disabled.</li> <li>• <b>Destination Only.</b> Collects destination MAC data. This option can be used in connection forwarding deployments.</li> <li>• <b>Destination and Source.</b> Collect mappings from destination and source MAC data. This option cannot be used in connection forwarding deployments.</li> <li>• <b>All.</b> Collect mappings for destination and source MAC data and data. It also collects data for connections that are <i>un-natted</i> (that is, connections that are not translated using Network Address Translation (NAT)). This option cannot be disabled in connection forwarding deployments.</li> </ul>

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling WCCP Groups

You can enable WCCP service groups in the Advanced Networking - WCCP Service Groups page.

WCCP enables you to redirect traffic that is not in the direct physical path between the client and the server. To enable WCCP, the HP EFS WAN Accelerator must join a service group at the router. A service group is a group of routers and HP EFS WAN Accelerators which define the traffic to redirect, and the routers and HP EFS WAN Accelerators the traffic goes through.

Enabling WCCP is *optional*.

---

**TIP:** You can also use the HP EFS WAN Accelerator Command Line Interface (CLI) to configure WCCP service groups. For detailed configuration information (including configuring the WCCP router), see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

---

---

**NOTE:** The following section assumes you are familiar with WCCP. For detailed information about WCCP, see the Cisco documentation Web site at <http://www.cisco.com/univercd/home/home.htm>.

---

### To enable a WCCP service group

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click WCCP Groups to display the Advanced Networking - WCCP Service Groups page.

Figure 2-37. Advanced Networking - WCCP Service Groups Page

Home

Setup

Reports

Logging

Help

Status: Healthy [config save required]

Logged in as: admin [logout]

Optimization Service

Host Settings

Advanced Networking

Asymmetric Routing

Connection Forwarding

Encryption

Fallover Settings

NetFlow

Peering Rules

QoS Classification

QoS Marking

Service Ports

Simplified Routing

WCCP Groups

Proxy File Service

Port Labels

Reports

Logging

Date & Time

Authentication

Licenses

Scheduled Jobs

Configuration Manager

Upgrade Software

Start/Stop Services

Reboot Appliance

Shutdown Appliance

Advanced Networking - WCCP Service Groups

Configure your WCCP v2 service groups.

Click on a service group to modify its settings.

General

Enable WCCP v2 Support

Multicast TTL: 1

Apply

Service Group ID	Priority	Weight	Scheme
No WCCP service groups.			

Remove Selected Groups

Add New Service Group:

Service Group ID:

Router IP:

Password:

Confirm Password:

Priority: 200

Weight: 180

Encapsulation Scheme: either

Add Group

Save

Reset

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<p><b>Enable WCCP v2 Support.</b> Select this box to enable WCCP v2 support on all groups added to the Service Group list.</p> <p><b>Multicast TTL.</b> Specify the TTL boundary for the WCCP protocol packets. The default value is 5.</p> <p><b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.</p>

HP STORAGEWORKS EFS WAN ACCELERATOR MANAGEMENT CONSOLE USER GUIDE

95

Control	Description
Add New Service Group	<p><b>Service Group ID.</b> Specify the service group identification number (from <b>0</b> to <b>255</b>). The service group ID is the number that is set on the router. A value of <b>0</b> specifies the standard <b>http</b> service group.</p> <p><b>Router IP.</b> Specify a multicast group IP address or a unicast router IP address. You can specify up to 32 routers. For information on adding additional routers to the group, see <a href="#">“Modifying WCCP Group Settings” on page 96</a>.</p> <p><b>Password/Confirm Password.</b> Optionally, you can assign a password to the HP EFS WAN Accelerator. This password must be the same password that is on the router. WCCP requires that all routers in a service group have the same password. Passwords are limited to 8 characters.</p> <p><b>Priority.</b> Specify the WCCP priority for traffic redirection. If a connection matches multiple service groups on a router, the router chooses the service group with the highest priority. The range is <b>0-255</b>. The default value is <b>200</b>.</p> <p><b>Weight.</b> Determine how often the traffic is redirected to a particular HP EFS WAN Accelerator. A higher weight redirects more traffic to that HP EFS WAN Accelerator. The ratio of traffic redirected to an HP EFS WAN Accelerator is equal to its weight divided by the sum of the weights of all the HP EFS WAN Accelerators in the same service group. For example, if there are two HP EFS WAN Accelerators in a service group and one has a weight of <b>100</b> and the other has a weight of <b>200</b>, the one with the weight <b>100</b> receives 1/3 of the traffic and the other receives 2/3 of the traffic. The range is <b>0-65535</b>. The default value corresponds to the number of TCP connections your appliance supports.</p> <p><b>NOTE:</b> To enable failover support for WCCP groups, define the service group weight to be <b>0</b> on the backup HP EFS WAN Accelerator. If one HP EFS WAN Accelerator has a weight <b>0</b>, but another one has a non-zero weight, the HP EFS WAN Accelerator with weight <b>0</b> does not receive any redirected traffic. If all the HP EFS WAN Accelerators have a weight <b>0</b>, the traffic is redirected equally among them.</p> <p><b>Encapsulation Scheme.</b> Specify the traffic forwarding and redirection scheme: Generic Routing Encapsulation (<b>gre</b>) or Layer-2 (<b>l2</b>) redirection. Specify <b>either</b> to use Layer-2 first; if Layer-2 is not supported, <b>gre</b> is used.</p> <p><b>Add Group.</b> Click <b>Add Group</b> to add the group to the Service Group list.</p> <p><b>Remove Selected Groups.</b> To remove an entry, select it and click <b>Remove Selected Groups</b>.</p>

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying WCCP Group Settings

You modify WCCP service group settings, add additional routers to a service group, and set flags for source and destination ports to redirect traffic (that is, the hash table settings) in the Advanced Networking - WCCP Service Group: <group ID> page.

Before you can modify WCCP service group settings, you must create a WCCP service group. For information on creating a WCCP service group, see [“Enabling WCCP Groups” on page 94](#).

For detailed information about hash table settings for WCCP, see the Cisco documentation Web site at <http://www.cisco.com/univercd/home/home.htm>.






## To modify WCCP service group settings

1. Click the Setup tab to display the Setup menu.
2. Click Advanced Networking to expand the Advanced Networking menu.
3. Click WCCP Groups to display the WCCP Service Groups page.
4. Click the service group ID in the Groups list to display Advanced Networking - WCCP Service Group: <Group ID> page.

**Figure 2-38.** Advanced Networking - WCCP Service Group: <Group ID> Page

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: admin [ logout ]

**Advanced Networking - WCCP Service Group: 123**  

 Configure the settings for service group 123. [\[ Return to Service Groups \]](#)

---

**Group Settings**

Password:

Confirm Password:

Priority:

Weight:

Encapsulation Scheme:

---

**Flags**

☐ Source IP Hash    ☒ Destination IP Hash

☐ Source Port Hash    ☐ Destination Port Hash

---

**Ports**

☒ Ports Disabled    ☐ Use Source Ports    ☐ Use Destination Ports   

**Port**

*No ports specified.*

**Add Port:**

---

**Routers**

**Router**

☐ 10.0.0.0

**Add Router IP:**

5. Use the controls to complete the configuration, as described in the following table.

Control	Description
Group Settings	<b>Password/Confirm Password.</b> Optionally, you can assign a password to the HP EFS WAN Accelerator. This password must be the same password that is on the router. WCCP requires that all routers in a service group have the same password. Passwords are limited to 8 characters.
	<b>Priority.</b> Specify the WCCP priority for traffic redirection. If a connection matches multiple service groups on a router, the router chooses the service group with the highest priority. The range is <b>0-255</b> . The default value is <b>200</b> .
	<b>Weight.</b> Determine how often the traffic is redirected to a particular HP EFS WAN Accelerator. A higher weight redirects more traffic to that HP EFS WAN Accelerator. The ratio of traffic redirected to an HP EFS WAN Accelerator is equal to its weight divided by the sum of the weights of all the HP EFS WAN Accelerators in the same service group. For example, if there are two HP EFS WAN Accelerators in a service group and one has a weight of <b>100</b> and the other has a weight of <b>200</b> , the one with the weight <b>100</b> receives 1/3 of the traffic and the other receives 2/3 of the traffic. The range is <b>0-65535</b> . The default value corresponds to the number of TCP connections your appliance supports.
	<b>NOTE:</b> To enable failover support for WCCP groups, define the service group weight to be <b>0</b> on the backup HP EFS WAN Accelerator. If one HP EFS WAN Accelerator has a weight <b>0</b> , but another one has a non-zero weight, the HP EFS WAN Accelerator with weight <b>0</b> does not receive any redirected traffic. If all the HP EFS WAN Accelerators have a weight <b>0</b> , the traffic is redirected equally among them.
	<b>Encapsulation Scheme.</b> Specify the traffic forwarding and redirection scheme: Generic Routing Encapsulation ( <b>gre</b> ) or Layer-2 ( <b>l2</b> ) redirection. Specify <b>either</b> to use Layer-2 first; if Layer-2 is not supported, <b>gre</b> is used.
	<b>Update Settings.</b> If you modify group settings, click <b>Update Settings</b> to apply the settings to WCCP groups in the Service Group list.
Flags	<b>Source IP Hash.</b> Specify this option to specify that the router hash the source IP address to determine traffic to redirect.
	<b>Destination IP Hash.</b> Specify this option to specify that the router hash the destination IP address to determine traffic to redirect. You can set one or more flags.
	<b>Source Port Hash.</b> Specify this option to specify that the router hash the source port to determine traffic to redirect. You can set one or more flags.
	<b>Destination Port Hash.</b> Specify this option to specify that the router hash the destination port to determine traffic to redirect. You can set one or more flags.
	<b>Update Flags.</b> Click <b>Update Flags</b> to apply your settings.
Ports	<b>Ports Disabled.</b> Select this option to turn off port matching.
	<b>Use Source Ports.</b> Select this option to redirect TCP traffic when the source port matches the port numbers in the port list.
	<b>Use Destination Ports.</b> Select this option to redirect TCP traffic when the destination port matches the port numbers in the Port list.
	<b>Apply.</b> Click <b>Apply</b> to apply the change to the Port list.
	<b>Add Port.</b> Specify the port number and click <b>Add Port</b> to add it to the Port list. You can add up to 7 ports.
	<b>Remove Selected Ports.</b> To remove an entry, select it and click <b>Remove Selected Ports</b> .

Control	Description
Routers	<p><b>Add Router IP.</b> Specify a multicast group IP address or a unicast router IP address and click <b>Add Router</b> to add it to the Router list. You can add up to 32 routers.</p> <p><b>Remove Selected Routers.</b> To remove an entry, select it and click <b>Remove Selected Routers</b>.</p>

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Enabling Proxy File Service

This section describes how to enable and configure the Proxy File Service (PFS) for the HP EFS WAN Accelerator. It includes the following sections:

- ◆ [“Enabling PFS,” next](#)
- ◆ [“Adding PFS Shares” on page 102](#)

## Enabling PFS

You can enable and configure PFS support in the Proxy File Service (PFS) - Configuration page.

---

**NOTE:** PFS is not supported on the Model 510.

---

PFS is an optional integrated virtual file server that allows you to store copies of files on the HP EFS WAN Accelerator with Windows file access, while creating several options for transmitting data between remote offices and centralized locations with improved performance and functions. PFS provides:

- ◆ LAN access to data residing across the WAN.
- ◆ Continuous access to files in the event of WAN disruption.
- ◆ Simplified branch infrastructure and backup architectures.

In v3.0 you no longer need to install the HP EFS Remote Copy Utility (RCU) service on the server to synchronize your PFS shares—all RCU functionality has been moved to the HP EFS WAN Accelerator. When you upgrade from v2.x to v3.x all your existing shares will be running as v2.x shares. If you have legacy shares (that is, shares created with Version v2.x software), you can convert your v2.x shares to v3.x shares in the Management Console.

For detailed information about PFS and when to enable it, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

Enabling PFS support is *optional*.

To enable PFS

1. Click the Setup tab to display the Setup menu.
2. Click Proxy File Service to display the Proxy File Service (PFS) - Configuration page.

Figure 2-39. Proxy File Service (PFS) - Configuration Page

Home

Setup

Reports

Logging

Help

Status: **Healthy** [ config save required ] [ restart required ]

Logged in as: **admin** [ logout ]

• Optimization Service

• Host Settings

• Advanced Networking

• Proxy File Service

• Configuration «

• Shares

• Port Labels

• Reports

• Logging

• Date & Time

• Authentication

• Licenses

• Scheduled Jobs

• Configuration Manager (1)

• Upgrade Software

• Start/Stop Services (1)

• Reboot Appliance

• Shutdown Appliance

Proxy File Service (PFS) - Configuration

Check and modify your Proxy File Service (PFS) configuration. Some notes:

The Proxy File Service can be disabled, enabled-and-stopped, or running. PFS needs to be enabled before it can be used.

Select either *Domain Settings* mode to join a domain, or *Local Workgroup Settings* mode to define a workgroup and add individual users. It is necessary to leave the domain/workgroup before switching between these modes.

Start Proxy File Service

Status: PFS stopped

Disable

Enable

Start

Domain / Local Workgroup Settings

Domain Settings

Local Workgroup Settings

Workgroup Name:

Status: In a workgroup

Leave

Join

Users

No users.

Remove

selected users

Add User:

User:

Password:

Password Confirm:

Add

Other PFS Settings

Security Signature Settings:

Enabled

Idle Connection Timeout:

minutes

Local Admin User Name:

administrator

Local Admin Password:

Local Admin Password Confirm:

Save

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Start Proxy File Service	<p><b>Enable/Disable.</b> Enable or disable PFS support. PFS must be enabled before it is configured. You must restart the HP EFS WAN Accelerator each time PFS is enabled or disabled.</p> <p>When you click <b>Enable</b>, the page refreshes displaying the Domain/Local Workgroup controls.</p> <p><b>Start/Stop.</b> Starts and stops the PFS service.</p> <p><b>NOTE:</b> You must restart the HP EFS WAN Accelerator service if you enable PFS support.</p>

Control	Description
Local Workgroup Settings	<p><b>Workgroup Name.</b> Specify a local workgroup name. If you configure PFS in Workgroup mode the HP EFS WAN Accelerator does not need to join a domain. Workgroup accounts are used by clients when they connect to the HP EFS WAN Accelerator to access PFS shares.</p> <p><b>NOTE:</b> PFS must be enabled and <b>Local Workgroup Settings</b> must be selected before you can set the Workgroup Name. After you have set a Workgroup Name click the <b>Join</b> button.</p> <hr/> <p><b>Join/Leave.</b> Click <b>Join</b> to join the workgroup; click <b>Leave</b> to leave the local workgroup.</p> <p><b>IMPORTANT:</b> If you are in Domain mode and have joined a domain you cannot change to workgroup mode until you leave the domain.</p> <hr/> <p><b>User.</b> Specify the login to create a local workgroup account so that users can connect to the HP EFS WAN Accelerator and to access PFS shares.</p> <hr/> <p><b>Password/Password Confirm.</b> Specify and confirm the user account password.</p> <hr/> <p><b>Add.</b> Click <b>Add</b> to add users to the local workgroup.</p> <hr/> <p><b>Remove.</b> To remove an entry, select it and click <b>Remove</b>.</p>
Domain Settings	<p><b>Fully-Qualified Domain Name/Realm.</b> The domain to which you want to make the proxy file server a member. Typically, this is your company domain name. PFS supports Windows 2000 domains.</p> <p><b>NOTE:</b> PFS does not support non-domain accounts other than Administrator accounts. If you create <b>Local</b> mode shares on a non-administrator account, your security permissions for the share will not be preserved on the origin server.</p> <hr/> <p><b>Primary DNS IP.</b> By default, this field displays the primary DNS IP set in the DNS Settings page. To modify this entry, click the IP address.</p> <hr/> <p><b>Domain Admin Login.</b> Specify the administrator login for the domain.</p> <hr/> <p><b>Domain Admin Password/Password Confirm.</b> Specify and confirm the domain administrator password.</p> <hr/> <p><b>Domain Controller Name.</b> Optionally, specify the domain controller names (that is, the host that provides user log in service in the domain). Typically, with Windows 2000 Active Directory Service domains, given a domain name, the system automatically retrieves the domain controller name. Enter the names in a comma-separated list.</p> <p><b>NOTE:</b> If you specify the domain controller name in high latency situations, it will reduce the time to join domain significantly.</p> <hr/> <p><b>Short Domain Name.</b> Optionally, specify a short domain name, if available. Typically, the short domain name is a sub-string of the realm. In rare situations, this is not the case, and you must explicitly specify it.</p> <hr/> <p><b>Join/Leave.</b> Click <b>Join</b> to join the domain or <b>Leave</b> to leave the domain.</p> <p><b>IMPORTANT:</b> If you are in Domain mode and have joined a domain you cannot change to workgroup mode until you leave the domain.</p> <hr/> <p><b>Cancel.</b> Click <b>Cancel</b> to cancel any current domain action that is in progress, such as joining or leaving a domain.</p>

Control	Description
Other PFS Settings	<p><b>Security Signature Settings.</b> Select one of the following settings:</p> <p><b>Enabled.</b> This setting supports any type of security signature setting requested by the client machine.</p> <p><b>Disabled.</b> This is the default setting. In this setting, PFS does not support clients with security signatures set to <b>Required</b>.</p> <p><b>Required.</b> In this setting, PFS supports clients with security signatures set to <b>Enabled</b> or <b>Required</b>.</p> <hr/> <p><b>Idle Connection Timeout.</b> Specify the number of minutes after which to time-out idle connections. If there is no read or write activity on a mapped PFS share on a client machine, then the TCP connection times out according to the value set and the client has to re-map the share.</p> <hr/> <p><b>Local Admin User Name.</b> Displays the local administrator user name—<b>administrator</b>. The local administrator account can be used to manage PFS files. You must use the correct syntax for the administrator login name (for example: <b>administrator@parent_realm</b>) even if you belong to a subdomain.</p> <p><b>NOTE:</b> PFS does not support non-domain accounts other than Administrator accounts. If you create <b>Local</b> mode shares on a non-administrator account, your security permissions for the share will not be preserved on the origin server.</p> <p><b>TIP:</b> To change the ACLs on a share hosted by PFS, first map it using the local administrator account.</p> <hr/> <p><b>Local Admin Password/Confirm.</b> Specify and confirm the local administrator password.</p> <hr/> <p><b>Save.</b> Click <b>Save</b> to save your settings permanently.</p>

## Adding PFS Shares

You create and manage PFS shares in the Proxy File Service - Shares page.

A share is the data volume exported by the origin server.

## To set PFS share parameters

1. Click the Setup tab to display the Setup menu.
2. Click Proxy File Service to expand the PFS menu.
3. Click Shares to display the Proxy File Service - Shares page.
4. Click **Add a new Proxy Share** to display the Proxy File Service (PFS) - Shares page.

**Figure 2-40. Proxy File Service - Shares Page**

Home : Setup : Reports : Logging : Help Status: **Healthy** Logged in as: admin [logout]

**Proxy File Service (PFS) - Shares**

Check and modify your Proxy File Service (PFS) shares.

Add a Proxy Share.

Local Name:

Remote Path:   
(Format is "\\servername\sharename")

Comment (optional):

Mode and Version: Broadcast Version 3

Account:

Password:

Password Confirm:

Incremental Sync Start Date and Time: 2006/07/26 (YYYY/MM/DD) 12:17:48 (HH:MM:SS)

Incremental Sync Interval: 720 Minutes

Full Sync Start Date and Time: 2006/07/26 (YYYY/MM/DD) 12:17:48 (HH:MM:SS)

Full Sync Interval: 10800 Minutes (Use "0" to disable full sync.)

Cancel Save

Local Name	Sharing	Syncing	Status	Last Sync Time	Last Sync Status	Actions
broadcast1	no	yes	Share idle	2006/07/21 12:44:08	Failed	-- Actions --
broadcast10	no	yes	Share idle	2006/07/21 12:43:48	Failed	-- Actions --

5. Use the controls to complete the configuration, as described in the following table.

Control	Description
Local Name	Specify the name that you assign to a share on the HP EFS WAN Accelerator. The maximum length is 80 characters.  <b>IMPORTANT:</b> The PFS share and the origin-server share name cannot contain Unicode characters. The Management Console does not support Unicode characters.
Remote Path	Specify the remote path of the origin file server where the share resides. You must use the Uniform Naming Convention (UNC) for the mapped drive for v3 shares. For example, \\<origin-file-server>\<local-name>  <b>IMPORTANT:</b> The PFS share and the origin-server share name cannot contain Unicode characters. The Management Console does not support Unicode characters.  <b>NOTE:</b> If you created your share with v2.x software, this value represents the name of the Windows server where the HP EFS Remote Copy Utility (RCU) is running. If the origin server is not the RCU server, you specify the remote path using the UNC format for the mapped drive. If the origin server is the same as the RCU server then you must type its full path including the drive letter, for example <b>C:\data</b> .
Comment	Optionally, specify a comment to help you identify the share.

Control	Description
Mode	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Broadcast.</b> The share originates on the origin server and a read-only copy is available as a share on the branch-office HP EFS WAN Accelerator. The data is updated periodically on the HP EFS WAN Accelerator with the data from the origin server. You specify when and how frequently updates (that is, synchronization) are to occur when you configure a share.</li> </ul> <p><b>IMPORTANT:</b> While performing a incremental synchronization for <b>Broadcast</b> mode share, if files are deleted on the server, they are not deleted on the HP EFS WAN Accelerator.</p> <p><b>IMPORTANT:</b> For <b>Broadcast</b> mode: if you are performing directory moves regularly (for example, <code>mv ./dir1/dir2 ./dir3/dir2</code>), incremental synchronization will not reflect these directory changes. You must perform a full synchronization more frequently to keep the PFS shares in synchronization with the remote site.</p> <ul style="list-style-type: none"> <li>• <b>Local.</b> After the HP EFS WAN Accelerator receives the initial copy, new data generated by clients is periodically synchronized to the origin server. The folder on the origin server essentially becomes a back-up folder of the share on the HP EFS WAN Accelerator. Users must not directly write to this folder on the origin server. You specify when and how frequently updates (that is, synchronization) are to occur when you configure a share.</li> </ul> <p><b>CAUTION:</b> In <b>Local</b> Mode, the HP EFS WAN Accelerator copy of the data is the master copy; do not make changes to the shared files from the origin server while in <b>Local</b> mode. Changes are propagated from the remote office hosting the share to the origin server.</p> <p><b>NOTE:</b> PFS does not support non-domain accounts other than Administrator accounts. If you create <b>Local</b> mode shares on a non-administrator account, your security permissions for the share will not be preserved on the origin server.</p> <ul style="list-style-type: none"> <li>• <b>Stand-Alone.</b> Provides the branch-office HP EFS WAN Accelerator with a one time working copy of data mapped from the origin server. You can specify a remote path to a directory on the origin server, creating a copy at the branch-office. This data is not synchronized back to the origin server. The stand-alone share is an initial and one-time only synchronization.</li> </ul>
Version	<p>Select one of the following software versions from the drop-down list. The controls change according to the version you choose. This value represents the version of the share that you want to create.</p> <ul style="list-style-type: none"> <li>• <b>Version 2.</b> Specify the server name and remote path for the share folder on the origin file server. With v2 you must have the RCU service running on a Windows server—this can be the origin file server or a separate server.</li> </ul> <p>HP recommends you upgrade your v2.x shares to 3.x shares so that you do not have to run the RCU on a server. For detailed information, see <a href="#">“Upgrading Shares from V2.x to V3.x” on page 107</a>.</p> <p><b>IMPORTANT:</b> If you have shares that were created with v2.x of the HP EFS WAN Accelerator software, the account that starts the RCU must have full permissions to the folder on the origin file server. Also, the log-in user for the RCU server (which is used for v2.x shares) and the share creation user for v3 shares must to be a member of the Administrators group, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).</p> <ul style="list-style-type: none"> <li>• <b>Version 3.</b> Specify the login, password, and remote path used to access the share folder on the origin file server. With v3, the RCU runs on the HP EFS WAN Accelerator—you do not need to install the RCU service on a Windows server.</li> </ul> <p><b>IMPORTANT:</b> Make sure the users are members of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).</p>



Control	Description
Version 2	<p><b>Server Name.</b> The server located in the data center which hosts the origin data volumes (folders).</p> <p><b>Port.</b> Specify the port for the server.</p>
Version 3	<p><b>Account.</b> Specify the fully qualified Windows login (including domain) to be used to access the shares folder on the origin file server. For example, <b>&lt;Domain&gt;\Administrator</b>.</p> <p><b>IMPORTANT:</b> Make sure the users are members of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).</p> <p><b>Password/Password Confirm.</b> Specify and confirm the password to be used to access the shares folder on the origin file server.</p>
Incremental Sync Schedule, Date and Time	<p>Specify the date and time that you want updates (synchronization) to start. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.</p> <p><b>IMPORTANT:</b> For <b>Local</b> mode, changes are synchronized from the HP EFS WAN Accelerator to the origin file server; <b>Broadcast</b> mode changes are synchronized from the origin file server to the HP EFS WAN Accelerator.</p> <p><b>IMPORTANT:</b> For <b>Broadcast</b> mode: if you are performing directory moves regularly (for example, <b>mv ./dir1/dir2 ./dir3/dir2</b>), incremental synchronization will not reflect these directory changes. You must perform a full synchronization more frequently to keep the PFS shares in synchronization with the remote site.</p>
Incremental Sync Interval	Specify the frequency of updates (synchronization) in minutes.
Full Sync Schedule, Date and Time	<p>Specify the date and time that you want updates (synchronization) to start. Use full synchronization if performance is not an issue. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.</p> <p><b>IMPORTANT:</b> For <b>Local</b> mode, changes are synchronized from the HP EFS WAN Accelerator to the file server; <b>Broadcast</b> mode changes are synchronized from the origin file server to the HP EFS WAN Accelerator.</p> <p><b>IMPORTANT:</b> For <b>Broadcast</b> mode: if you are performing directory moves regularly (for example, <b>mv ./dir1/dir2 ./dir3/dir2</b>), incremental synchronization will not reflect these directory changes. You must perform a full synchronization more frequently to keep the PFS shares in synchronization with the remote site.</p>
Full Sync Interval	Specify the interval of updates (synchronization) in minutes.

6. Click **Save** to write your changes to disk or **Cancel** to cancel your settings.

After you save your share settings the share is added to the Shares list.

---

**NOTE:** The PFS service must be started to add a share. To start the PFS service, click **Start** in the Proxy File Service (PFS) - Configuration page. For details, see [“To enable PFS” on page 100](#).

---

## Enabling and Synchronizing Shares

After you have configured your PFS shares, you must perform the initial synchronization and enable your shares in the Proxy File Services (PFS) - Shares Details page.

When you perform the initial synchronization of the share, a copy of the data is downloaded from the origin server to the HP EFS WAN Accelerator. The HP EFS WAN Accelerator also configures the share for automatic synchronization according to the parameters you specified previously.

When you enable sharing for the first time, the share is made available to users for mounting. Users can map the mounted share using standard Windows mapping procedures. For example, map a network drive using the following format:

```
\\<appliance name or primary interface IP address>\<name of share>
```

### To initialize and enable a share

1. Click the Setup tab to display the Setup menu.
2. Click Proxy File Service to expand the PFS menu.
3. Click Shares to display the Proxy File Service - Shares page.
4. Click the Local Name of the share that you want to initialize or synchronize in the Shares list to display the Proxy File Service (PFS) - Shares Details page.

**Figure 2-41.** Proxy File Service (PFS) - Shares Details Page

The screenshot displays the 'Proxy File Service (PFS) - Shares' details page. The left sidebar contains navigation links for various services and settings. The main content area is titled 'Proxy File Service (PFS) - Shares' and includes a status indicator 'Healthy'. Below the title, there is a section for 'Edit Proxy Share \\gen-sh87\local1:' with configuration and current status details.

**Configuration**

- Local Name: local1
- Version: 3
- Remote Path: \\10.11.61.67\share1

**Current Status**

- Current Status: START\_SYNC in progress since Wed Jul 26 13:07:00 2006
- Last Successful Sync: 2006/07/26 13:06:00
- Last Sync Status: Succeeded

**Form Fields:**

- Comment (optional): [Text input field]
- Mode: [Dropdown menu, currently set to Local]
- Sharing Enable: [Checkbox, unchecked]
- Synding Enable: [Checkbox, unchecked]
- Account: [Text input field, set to Administrator]
- Password: [Text input field]
- Password Confirm: [Text input field]
- Incremental Sync Start Date and Time: [Date/Time picker, set to 2006/07/20 08:37:06]
- Incremental Sync Interval: [Text input field, set to 1 Minutes]
- Full Sync Start Date and Time: [Date/Time picker, set to 2006/07/20 08:37:06]
- Full Sync Interval: [Text input field, set to 0 Minutes (Use "0" to disable full sync.)]

**Buttons:** Cancel, Save

**Shares List Table:**

Local Name	Sharing	Synding	Status	Last Sync Time	Last Sync Status	Actions
broadcast1	no	yes	Share idle	2006/07/26 13:11:00	Succeeded	-- Actions --

5. Click **Syncing Enable** to download the initial copy of the share from the origin server to the HP EFS WAN Accelerator and to configure the share for automatic synchronization.

6. Click **Sharing Enable** to make the share available to end users for mounting. End users will be able to read the share by mapping to the mounted share (for example, \\HP EFS WAN Accelerator\share1).

After you enable sharing, you can map this share from your machine by typing: \\<HP EFS WAN Accelerator or primary interface IP address>\<name of share>

7. Click **Save** to write your changes to disk or **Cancel** to cancel your settings.

---

**NOTE:** When performing the initial synchronization, or when changing large amounts of data, your bandwidth utilization and other graphs may show pockets of inactivity. This is by design.

---

## Upgrading Shares from V2.x to V3.x

When you upgrade to v3.x software, all your existing shares will be running as v2.x shares.

In v3.0 you no longer need to install the HP EFS Remote Copy Utility (RCU) service on the server for synchronization purposes—all RCU functionality has been moved to the HP EFS WAN Accelerator.

If you have legacy shares (that is, shares created with Version 2.x software), you must upgrade your v2.x shares to v3.x shares in the Management Console.

---

**IMPORTANT:** HP recommends that you convert your v2.x shares to v3.x shares. HP recommends you do not configure a mixed system of PFS shares, that is v2.x shares and v3.x shares.

---

When you upgrade your shares you must specify the remote path for the share. The format depends on the path name:

- ◆ If you created your share with v2.x software, this value represents the name of the Windows server where the RCU is running. If the remote path share contains a drive letter, then you must provide a new remote path in UNC format that points to the same directory. For example, if the remote path was **c:\data\eng** on a server called **granite**. To upgrade, you must log in to **granite**, and make **c:\data\eng** a shared directory, with the name **eng**. In the Management Console, you specify **\\granite\eng** as your new remote path for the v3.x upgrade.
- ◆ If the remote path share is in UNC format, you simply copy that path to the **Remote Path** field.

## To upgrade your share

1. Click the Setup tab to display the Setup menu.
2. Click Proxy File Service to expand the PFS menu.
3. Click Shares to display the Proxy File Service - Shares page.
4. In the Shares list click the share name that you want to upgrade. The Proxy File Service (PFS) - Shares Details page appears.

**Figure 2-42. Proxy File Service (PFS) - Shares Details Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy**    Logged in as: **admin** [logout]

- Optimization Service
- Host Settings
- Advanced Networking
- **Proxy File Service**
  - Configuration
  - **Shares** «
- Port Labels
- Reports
- Logging
- Date & Time
- Authentication
- Licenses
- Scheduled Jobs

- Configuration Manager
- Upgrade Software

- Start/Stop Services
- Reboot Appliance
- Shutdown Appliance

### Proxy File Service (PFS) - Shares

Check and modify your Proxy File Service (PFS) shares.

Edit Proxy Share **\\meow-mix\pfsTortureB**:

#### Configuration

Local Name: pfsTortureB  
Version: 2  
Server Name: dfs1  
Remote Path: c:\data\pfs-torture-b

#### Current Status

Current Status: Share idle  
Last Successful Sync: 2006/07/26 13:53:00  
Last Sync Status: Succeeded

Comment (optional):

Mode: Broadcast

Sharing Enable: ☒

Syncing Enable: ☒

Server Port:

Incremental Sync Start Date and Time:  (YYYY/MM/DD)  (HH:MM:SS)  
Incremental Sync Interval:  Minutes  
Full Sync Start Date and Time:  (YYYY/MM/DD)  (HH:MM:SS)  
Full Sync Interval:  Minutes (Use "0" to disable full sync.)  
Upgrade to Version 3 on Save: ☐

Local Name	Sharing	Syncing	Status	Last Sync Time	Last Sync Status	Actions
field_kit	no	no	Share idle	2005/11/08 13:13:44	Failed	-- Actions --

5. Click **Upgrade to Version 3 on Save**. The page refreshes with additional controls necessary to configure v3.
6. Use the controls to complete the configuration, as described in the following table.

Control	Description
Account	Specify the fully qualified Windows login (including domain) to be used to access the shares folder on the origin file server. For example, <b>&lt;Domain&gt;\Administrator</b> .  <b>IMPORTANT:</b> Make sure the users are members of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).

Control	Description
Password/Password Confirm	Specify and confirm the password to be used to access the shares folder on the origin file server.
Remote Path	<p>Specify the remote path of the origin file server where the share resides. You must use the Uniform Naming Convention (UNC) for the mapped drive for Version 3 shares. For example, \\&lt;<b>origin-file-server</b>&gt;\&lt;<b>local-name</b>&gt;</p> <p><b>IMPORTANT:</b> The PFS share and the origin-server share name cannot contain Unicode characters. The Management Console does not support Unicode characters.</p> <p><b>NOTE:</b> If you created your share with v2.x software, this value represents the name of the Windows server where the HP EFS Remote Copy Utility (RCU) is running. If the origin server is not the RCU server, you specify the remote path using the UNC format for the mapped drive. If the origin server is the same as the RCU server then you must type its full path including the drive letter, for example <b>C:\data</b>.</p>

- Click **Save** to save your settings permanently or click **Cancel** to cancel your settings.

## Modifying Share Settings

You can modify your share settings in the Proxy File Service (PFS) - Shares Details page.

## To modify share settings

1. Click the Setup tab to display the Setup menu.
2. Click Proxy File Service to expand the PFS menu.
3. Click Shares to display the Proxy File Service - Shares page.
4. In the Shares list click the share name that you want to modify. The Proxy File Service (PFS) - Shares page is updated with the share name and current status displayed.

Figure 2-43. Proxy File Service (PFS) - Shares Page

Home : Setup : Reports : Logging : Help Status: **Healthy** Logged in as: **admin** [logout]

**Proxy File Service (PFS) - Shares**

Check and modify your Proxy File Service (PFS) shares.

Edit Proxy Share **\\gen-sh87\\local1:**

**Configuration**

Local Name: local1  
Version: 3  
Remote Path: \\10.11.61.67\\share1

**Current Status**

Current Status: START\_SYNC in progress since Wed Jul 26 13:07:00 2006  
Last Successful Sync: 2006/07/26 13:06:00  
Last Sync Status: Succeeded

Comment (optional):

Mode:

Sharing Enable: ☐

Syncing Enable: ☐

Account:

Password:

Password Confirm:

Incremental Sync Start Date and Time:  (YYYY/MM/DD)  (HH:MM:SS)

Incremental Sync Interval:  Minutes

Full Sync Start Date and Time:  (YYYY/MM/DD)  (HH:MM:SS)

Full Sync Interval:  Minutes (Use "0" to disable full sync.)

Local Name	Sharing	Syncing	Status	Last Sync Time	Last Sync Status	Actions
broadcast1	no	yes	Share idle	2006/07/26 13:11:00	Succeeded	-- Actions --

5. Use the controls to modify the configuration, as described in the following table.

Control	Description
Comment	Optionally, specify a comment to help you identify the share.
Mode	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Broadcast.</b> The share originates on the origin server and a read-only copy is available as a share on the branch-office HP EFS WAN Accelerator. The data is updated periodically on the HP EFS WAN Accelerator with the data from the origin server. You specify when and how frequently updates (that is, synchronization) are to occur when you configure a share.</li> </ul> <p><b>IMPORTANT:</b> For <b>Broadcast</b> mode: if you are performing directory moves regularly (for example, <b>mv ./dir1/dir2 ./dir3/dir2</b>), incremental synchronization will not reflect these directory changes. You must perform a full synchronization more frequently to keep the PFS shares in synchronization with the remote site.</p> <p><b>IMPORTANT:</b> While performing an incremental synchronization for <b>Broadcast</b> mode share, if files are deleted on the server, they are not deleted on the HP EFS WAN Accelerator.</p> <ul style="list-style-type: none"> <li>• <b>Local.</b> After the HP EFS WAN Accelerator receives the initial copy, new data generated by clients is periodically synchronized to the origin server. The folder on the origin server essentially becomes a back-up folder of the share on the HP EFS WAN Accelerator. Users must not directly write to this folder on the origin server. You specify when and how frequently updates (that is, synchronization) are to occur when you configure a share.</li> </ul> <p><b>CAUTION:</b> In <b>Local</b> Mode, the HP EFS WAN Accelerator copy of the data is the master copy; do not make changes to the shared files from the origin server while in <b>Local</b> mode. Changes are propagated from the remote office hosting the share to the origin server.</p> <p><b>NOTE:</b> PFS does not support non-domain accounts other than Administrator accounts. If you create <b>Local</b> mode shares on a non-administrator account, your security permissions for the share will not be preserved on the origin server.</p> <ul style="list-style-type: none"> <li>• <b>Stand-Alone.</b> Provides the branch-office HP EFS WAN Accelerator with a one time working copy of data mapped from the origin server. You can specify a remote path to a directory on the origin server, creating a copy at the branch-office. This data is not synchronized back to the origin server. The stand-alone share is an initial and one-time only synchronization.</li> </ul>
Version 2	<b>Port.</b> Specify the port for the server.
Version 3	<p><b>Account.</b> Specify the fully qualified Windows login (including domain) to be used to access the shares folder on the origin file server. For example, <b>&lt;Domain&gt;\Administrator</b>.</p> <p><b>IMPORTANT:</b> Make sure the users are members of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).</p> <p><b>Password/Password Confirm.</b> Specify and confirm the password to be used to access the shares folder on the origin file server.</p>
Incremental Sync Schedule, Date and Time	<p>Specify the date and time that you want updates (synchronization) to start. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.</p> <p><b>IMPORTANT:</b> For <b>Local</b> mode, changes are synchronized from the HP EFS WAN Accelerator to the origin file server; <b>Broadcast</b> mode changes are synchronized from the origin file server to the HP EFS WAN Accelerator.</p>

Control	Description
Incremental Sync Interval	Specify the frequency of updates (synchronization) in minutes.
Full Sync Schedule, Date and Time	Specify the date and time that you want updates to start. Use full synchronization if performance is not an issue. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the HP EFS WAN Accelerator. Subsequent synchronizations are based on the synchronization interval.  <b>IMPORTANT:</b> For <b>Local</b> mode, changes are synchronized from the HP EFS WAN Accelerator to the file server; <b>Broadcast</b> mode changes are synchronized from the origin file server to the HP EFS WAN Accelerator.
Full Sync Interval	Specify the interval of updates (synchronization) in minutes.

- Click **Save** to save your settings permanently or click **Cancel** to cancel your settings.

## Performing Manual Actions on Shares

You can verify a share, perform a full synchronization, cancel an operation, or delete a share in the Shares list. The shares list appears on the Proxy File Service (PFS) - Shares page and the Proxy File Service (PFS) - Shares Details page.

### To perform manual actions on shares

- Click the Setup tab to display the Setup menu.
- Click Proxy File Service to expand the PFS menu.
- Click Shares to display the Proxy File Service - Shares page.

**Figure 2-44.** Proxy File Service - Shares Page

Home : Setup : Reports : Logging : Help    Status: **Healthy**    Logged in as: admin [logout]

• Optimization Service  
• Host Settings  
• Advanced Networking  
• Proxy File Service ▾  
  • Configuration  
  • Shares «

• Port Labels  
• Reports  
• Logging  
• Date & Time  
• Authentication  
• Licenses  
• Scheduled Jobs

• Configuration Manager

• Upgrade Software

• Start/Stop Services  
• Reboot Appliance  
• Shutdown Appliance

### Proxy File Service (PFS) - Shares

💡 Check and modify your Proxy File Service (PFS) shares.

Add a new Proxy Share

Local Name	Sharing	Syncing	Status	Last Sync Time	Last Sync Status	Actions
broadcast1	no	yes	Share idle	2006/07/21 12:44:08	Failed	-- Actions --
broadcast10	no	yes	Share idle	2006/07/21 12:43:48	Failed	-- Actions --
broadcast11	no	yes	Share idle	2006/07/21 12:41:43	Failed	-- Actions --
broadcast12	no	yes	Share idle	2006/07/21 12:41:48	Failed	-- Actions --
broadcast13	no	yes	Share idle	2006/07/21 12:42:49	Failed	-- Actions --
broadcast14	no	yes	Share idle	2006/07/21 12:43:42	Failed	-- Actions --
broadcast15	no	yes	Share idle	2006/07/21 12:42:13	Failed	-- Actions --
broadcast16	no	yes	Share idle	2006/07/21 12:42:22	Failed	-- Actions --
broadcast17	no	yes	Share idle	2006/07/21 12:41:28	Failed	-- Actions --
broadcast18	no	yes	Share idle	2006/07/21 12:43:38	Failed	-- Actions --
broadcast19	no	yes	Share idle	2006/07/21 12:44:12	Failed	-- Actions --
broadcast2	no	yes	Share idle	2006/07/21 12:41:38	Failed	-- Actions --
broadcast20	no	yes	Share idle	2006/07/21 12:43:03	Failed	-- Actions --
broadcast21	no	yes	Share idle	2006/07/21 12:44:23	Failed	-- Actions --
broadcast22	no	yes	Share idle	2006/07/21 12:41:32	Failed	-- Actions --
broadcast23	no	yes	Share idle	2006/07/21 12:41:54	Failed	-- Actions --



4. Select one of the following actions for the share, as described in the following table.

Control	Description
Actions	<p>Select one of the following actions from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Start Verify.</b> Generates a list of the differences between the share on the HP EFS WAN Accelerator and the origin file server. The first time you synchronize a share the data comes from the origin file server. A list of differences is available in the PFS Shares Status report.</li> <li>• <b>Start Full Sync.</b> Allows you to immediately synchronize the share and its corresponding remote share on the origin file server. You may select <b>Start Full Sync</b> at any time to manually synchronize a share.</li> <li>• <b>Cancel Action.</b> Cancels the synchronization process.</li> <li>• <b>Delete Share.</b> Deletes the selected share.</li> </ul>

## Creating Port Labels

This section describes how to create port labels. It includes the following sections:

- ◆ [“Creating Port Labels” on page 113](#)
- ◆ [“Modifying Ports in a Port Label” on page 115](#)

## Creating Port Labels

You create port labels in the Port Labels page. Port labels are names given to sets of port numbers. You use port labels to simplify configuration and reporting tasks you perform with the Management Console. For example, you can create port labels to define a set of ports for which the same in-path, load-balancing, or QoS rules apply.

The HP EFS WAN Accelerator automatically discovers all the ports in the system that have traffic. The discovered port along with a label (if one exists) is added to the Traffic Summary report. If a label does not exist then an **unknown** label is added to the discovered port.

If you want to change the **unknown** label to a name representing the port, you must add the port with new label. All statistics for this new port label are preserved from the time the port was discovered.

The following tables summarizes the port labels that are provided by default.

Port Type	Description and Ports
Interactive	Automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell).
RBT-Proto	Specifies well-known ports used by the system: <b>7800-7801</b> (in-path), <b>7810</b> (out-of-path), <b>7820</b> (failover), <b>7850</b> (connection forwarding), <b>7860</b> (Interceptor appliance).
Secure	Automatically passes through traffic on secure ports (for example, <b>ssh</b> , <b>https</b> , and <b>smtps</b> ).

If you do not want to automatically forward traffic on these ports, you must delete the Interactive and Secure in-path rules. For detailed information, see “[Setting In-Path Rules](#)” on page 25.

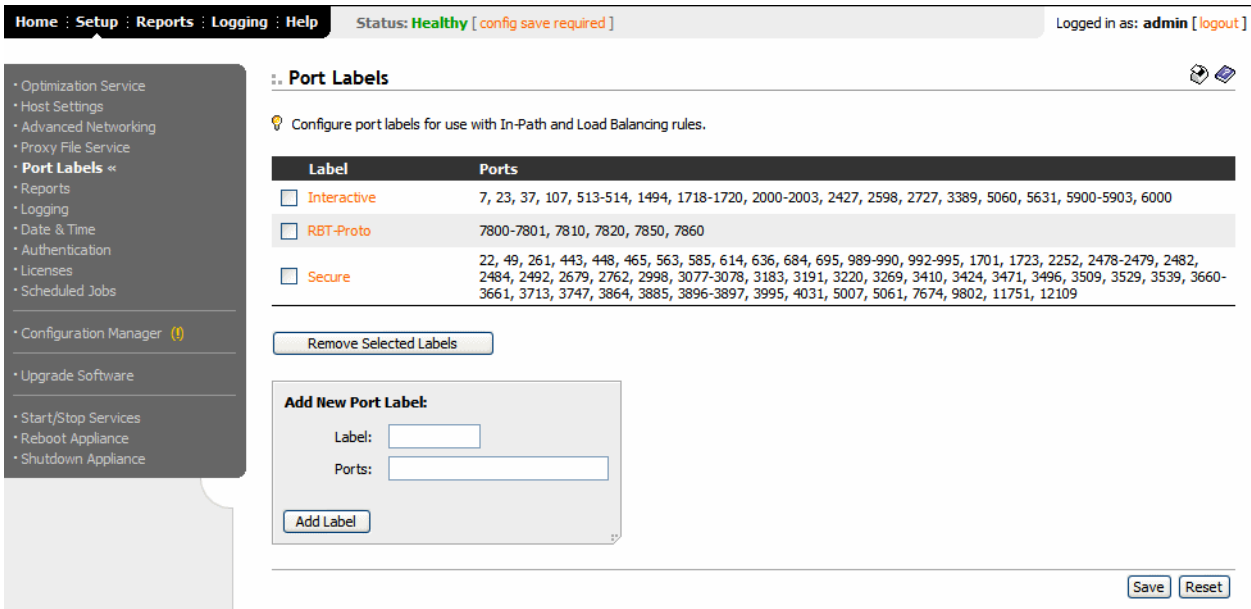
For information on common port assignments, see [Appendix A, “HP EFS WAN Accelerator Ports.”](#)

This feature is *optional*.

To create a port label

1. Click the Setup tab to display the Setup menu.
2. Click Port Labels to display the Port Labels page.

Figure 2-45. Port Labels Page



3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Port Label	<b>Label.</b> Specify the label name. The following rules apply:
	<ul style="list-style-type: none"><li>• Port labels are not case sensitive and can be any string consisting of letters, the underscore ( _ ), or the hyphen ( - ). There cannot be spaces in port labels.</li><li>• The fields in the various rule pages of the Management Console that take a physical port number also take a port label.</li><li>• To avoid confusion, do not use a number for a port label.</li><li>• Port labels that are used in in-path and other rules, such as QoS, and peering rules cannot be deleted.</li><li>• Port label changes (that is, adding and removing ports inside a label) are applied immediately by the rules that use the port labels that you have modified.</li></ul>
	<b>Ports.</b> Specify a comma-separated list of port numbers.
	<b>Add Label.</b> Click <b>Add Peer</b> to add a neighbor to the peer list.
	<b>Remove Selected Labels.</b> To remove an entry, select it and click <b>Remove Selected Labels</b> .

4. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying Ports in a Port Label

### To modify ports in a port label

You can add or delete ports associated with a port label in the Port Label: <Port Label Name> page.

1. Click the Setup tab to display the Setup menu.
2. Click Port Labels to display the Port Labels page.
3. Click the port label name in the Port Labels list to display the Port Label - <Port Label Name> page.

**Figure 2-46.** Port Label: <Port Label Name> Page

4. Under Ports, add or delete ports in the **Ports** text box.
5. Click **Update Ports** to save your settings. Click **Cancel** to cancel your changes.
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Report Parameters

This section describes how to set parameters to generate alarm and error reports. It includes the following sections:

- ◆ “Setting Alarm Parameters,” next
- ◆ “Setting Email Notification” on page 117
- ◆ “Setting SNMP Parameters” on page 119
- ◆ “Setting SNMP Trap Receivers” on page 120
- ◆ “Setting Monitored Ports” on page 121

## Setting Alarm Parameters

### To set alarm parameters

You can set alarms in Reports - Alarm Settings page.

Enabling alarms is *optional*.

1. Click the Setup tab to display the Setup menu.
2. Click Reports to display the Reports - Alarm Settings page.

**Figure 2-47. Reports - Alarm Settings Page**

The screenshot shows the 'Reports - Alarm Settings' page. At the top, there is a navigation bar with 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The 'Reports' tab is active. Below the navigation bar, the status is 'Healthy' with a note '[config save required]'. The user is logged in as 'admin' with a 'logout' link. On the left, a sidebar menu lists various settings, with 'Reports' expanded to show 'Alarm Settings'. The main content area is titled 'Reports - Alarm Settings' and contains the following sections:

- CPU Alarm:** A checkbox 'Raise Alarm When CPU Utilization Reaches:' is checked. Below it are input fields for 'Rising Threshold' (set to 90) and 'Reset Threshold' (set to 70).
- Data Store Alarm:** A checkbox 'Send email if stale data replaced by fresh data is less than 1 day(s) old' is unchecked.
- Warning Temperature Alarm:** A checkbox 'Raise Alarm When Temperature (°C) Reaches:' is checked. Below it are input fields for 'Rising Threshold' (set to 70) and 'Reset Threshold' (set to 67).
- Additional Alarms:** Four checkboxes are listed:
  - 'Raise Alarm When Network Interface Duplex Errors are Detected' (checked)
  - 'Raise Alarm When Network Interface Link Errors are Detected' (unchecked)
  - 'Raise Alarm When Extended Memory Paging Activity is Detected' (checked)
  - 'Raise Alarm If a Software Version Mismatch is Detected in the Network' (checked)

At the bottom right of the page, there are three buttons: 'Apply', 'Save', and 'Reset'.

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
CPU Alarms	<p><b>Raise Alarm When CPU Utilization Reaches.</b> Specify this option to trigger an alarm if the average and peak threshold for the Central Processing Unit (CPU) utilization is exceeded. When an alarm reaches the rising threshold, it is activated; when it reaches the lowest or reset threshold, it is reset. After an alarm is triggered, it is not triggered again until it has fallen below the reset threshold.</p> <p>This alarm is enabled by default, with a rising threshold of 90% and a reset threshold of 70%.</p> <p><b>Rising Threshold.</b> Specify rising value CPU utilization.</p> <p><b>Reset Threshold.</b> Specify reset value for CPU utilization.</p>
Data Store Alarm	<p><b>Send email if stale data replaced by fresh data is less than __ day(s) old.</b> Specify this option to trigger an alarm if data in the data store is replaced with new data before the time period specified.</p>

Control	Description
Warning Temperature Alarm	<p><b>Raise Alarm When Temperature (°C) Reaches.</b> Specify this option to trigger an alarm when the CPU temperature exceeds the rising threshold. When the CPU returns to the reset threshold, the rising alarm is cleared. When the CPU returns to the reset threshold, the rising alarm is cleared. The default value for the rising threshold temperature is 70° C; the default reset threshold temperature is 67° C.</p> <hr/> <p><b>Rising Threshold.</b> Specify the rising temperature (° C).</p> <hr/> <p><b>Reset Threshold.</b> Specify the reset temperature (° C).</p>
Additional Alarms	<p><b>Raise Alarm When Network Interface Duplex Errors are Detected.</b> Specify this option to trigger an alarm if the system has encountered a large number of packet errors in your network. Make sure the speed and duplex settings on your HP EFS WAN Accelerator match the settings on your switch and router.</p> <p>This alarm is enabled by default.</p> <hr/> <p><b>Raise Alarm When Network Interface Link Errors are Detected.</b> Specify this option to trigger an Simple Network Management Protocol (SNMP) trap, email, and alarm notification when a link goes down. This alarm is disabled by default.</p> <p>For WAN/LAN interfaces, an alarm is only triggered if in-path support is enabled for that WAN/LAN pair.</p> <hr/> <p><b>Raise Alarm When Extended Memory Paging Activity is Detected.</b> Specify this option to trigger the memory paging alarm. If 100 pages are swapped every couple of hours, the HP EFS WAN Accelerator is functioning properly. If thousands of pages are swapped every few minutes, contact HP Technical Support.</p> <p>This alarm is enabled by default.</p> <hr/> <p><b>Raise Alarm If a Software Version Mismatch is Detected in the Network.</b> Specify this option to trigger an alarm if there is a mismatch between software versions in the HP EFS WAN Accelerator system.</p> <p>This alarm is enabled by default.</p>

- Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Email Notification

You can set email notification parameters for events and failures in the Reports - Notification page.

By default email addresses are not specified for event and failure notification.

## To set event and failure email notification

1. Click the Setup tab to display the Setup menu.
2. Click Reports expand the Reports menu.
3. Click Notification to display the Reports - Notification page.

**Figure 2-48. Reports - Notification Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy**    Logged in as: **admin** [ [logout](#) ]

**Reports - Notification**

Configure your alarm notification settings.

**Events**

☒ Report Events to SNMP Agent

☒ Report Events via Email

Email Addresses: (separate each address by a space)

**Failures**

☒ Report Failures via Email

Email Addresses: (separate each address by a space)

**SMTP Server for Emails**

SMTP Server:

SMTP Port:

[Apply](#) [Save](#) [Reset](#)

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Events	<b>Report Events to SNMP Agent.</b> Specify this option to report activity to an SNMP agent. To complete SNMP settings, see <a href="#">“Setting SNMP Parameters” on page 119</a> .
	For detailed information about SNMP traps sent to configured servers, see <a href="#">“SNMP Traps” on page 210</a> .
	<b>Report Events via Email.</b> Specify this option to report events via email.
Failures	<b>Email Addresses.</b> Specify a space-separated list of email address to which to send notification messages.
	<b>Report Failures via Email.</b> Specify this option to report failures via email.
	<b>Email Addresses.</b> Specify a space-separated list of email address to which to send notification messages.

Control	Description
SMTP Server	<p><b>SMTP Server.</b> Specify a valid Simple Mail Transfer Protocol (SMTP) server. External DNS and external access for SMTP traffic is required for this feature to function.</p> <p><b>IMPORTANT:</b> Make sure you provide a valid SMTP server to ensure that the users you specify receive email notifications for events and failures.</p> <p><b>SMTP Port.</b> Specify a port number for the SMTP server.</p>

- Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting SNMP Parameters

You set SNMP parameters in the Reports - SNMP Settings page.

By default SNMP parameters are not configured.

### To set SNMP parameters

- Click the Setup tab to display the Setup menu.
- Click Reports expand the Reports menu.
- Click SNMP Settings to display the Reports - SNMP Settings page.

**Figure 2-49.** Reports - SNMP Settings Page

- Use the controls to complete the configuration, as described in the following table.

Control	Description
System Contact	Specify the user name for the SNMP contact.

Control	Description
System Location	Specify the physical location of the router.
Read Only Community Name	Specify a string to identify the read-only community. For example: <b>public</b> .

- Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting SNMP Trap Receivers

You set SNMP traps in the Reports - SNMP Trap Receivers page.

Traps are messages sent by an SNMP agent that indicate the occurrence of an event.

For detailed information about SNMP traps sent to configured servers, see “[SNMP Traps](#)” on page 210.

The default setup does not complete SNMP traps.

### To set an SNMP trap

- Click the Setup tab to display the Setup menu.
- Click Reports expand the Reports menu.
- Click SNMP Trap Receivers to display the Reports - SNMP Trap Receivers page.

**Figure 2-50.** Reports - SNMP Trap Receivers Page

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: **admin** [ logout ]

**Reports - SNMP Trap Receivers**

Configure SNMP trap receivers if you would like to receive SNMP traps when alarms are triggered.

Trap Receiver	Community	Type	Enabled
No trap receivers.			

Remove Selected Receivers    Enable    Disable

**Add New Trap Receiver:**

Receiver IP:

Community:

Type: **v1**

Enabled: **True**



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Trap Receiver	<b>Receiver IP.</b> Specify the IP address for the SNMP trap. For detailed information about SNMP traps sent to configured servers, see <a href="#">“SNMP Traps” on page 210</a> .
	<b>Community.</b> Specify the SNMP community name.
	<b>Type.</b> Select <b>v1</b> or <b>v2c</b> from the drop-down list to specify the SNMP software version.
	<b>Enabled.</b> Select <b>True</b> to enable or <b>False</b> to disable the trap receiver.
	<b>Add Trap Receiver.</b> Click <b>Add Trap Receiver</b> to add the configuration to the Trap Receiver list.
	<b>Remove Selected Receivers.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Receivers</b> .

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Monitored Ports

You set TCP ports you want to monitor in the Reports - Monitored Ports page.

By default, traffic is monitored on ports 21 (FTP), 80 (HTTP), 139 (CIFS:NetBIOS), 445 (CIFS:TCP), 1433 (SQL:TDS), Radius (1812), TACACS+ (49), and 7830 (MAPI).

## To set monitored ports

1. Click the Setup tab to display the Setup menu.
2. Click Reports expand the Reports menu.
3. Click Monitored Ports to display the Reports - Monitored Ports page.

**Figure 2-51. Reports - Monitored Ports Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: admin [ logout ]

**Reports - Monitored Ports**

Configure the TCP ports for which statistics must be kept.  
These ports will always be monitored in addition to any ports the system auto discovers.

Monitored Port	Description
<input type="checkbox"/> 21	FTP
<input type="checkbox"/> 80	HTTP
<input type="checkbox"/> 139	CIFS:NetBIOS
<input type="checkbox"/> 445	CIFS:TCP
<input type="checkbox"/> 1433	SQL:TDS
<input type="checkbox"/> 7830	MAPI

Remove Selected Ports    Update All Ports

**Add New Port to Monitor:**

Port:

Description:

Add Port

**Set Maximum number of ports to Monitor:**

Maximum ports:

Set

Save    Reset

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New Port to Monitor	<b>Port.</b> Specify the port to be monitored.
	<b>Description.</b> Specify a description for the monitoring activity.
	<b>Add Port.</b> Click <b>Add Port</b> to add the port to the Monitored Port list.
	<b>Remove Selected Ports.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Ports</b> .
Set Maximum Number of Ports to Monitor	<b>Update All Ports.</b> To change the description of a port, edit the description and click <b>Update All Ports</b> .
	<b>Maximum Ports.</b> Specify the maximum number of ports to monitor. This option restricts the number of ports
	<b>Set.</b> Click <b>Set</b> to restrict the number of ports that the HP EFS WAN Accelerator monitors.

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Logging Options

This section describes how to set local and remote logging for the HP EFS WAN Accelerator. It includes the following sections:

- ◆ “Setting Local Logging,” next
- ◆ “Setting Remote Logging” on page 124

### Setting Local Logging

You set up local logging in the Logging - General Settings page.

#### To set up local logging

- Click the Setup tab to display the Setup menu.
- Click Logging to display the Logging - General Settings page.

Figure 2-52. Logging - General Settings Page

The screenshot displays the 'Logging - General Settings' page in the HP EFS WAN Accelerator Management Console. The top navigation bar shows 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy' with a note '[config save required]'. The user is logged in as 'admin' with a 'logout' link. The left sidebar lists various configuration options, with 'Logging' expanded to show 'General Settings' and 'Remote Log Servers'. The main content area is titled 'Logging - General Settings' and includes a lightbulb icon with the text 'Configure your local logging settings.' Below this, there are three sections: 'Log Filtering' with a 'Minimum Severity' dropdown set to 'Info'; 'Log Rotation' with radio buttons for 'Rotate every' (set to 'Day') and 'Rotate when log reaches' (set to '16 MB'), and a 'Keep at most' field set to '10 log file(s)'; and 'Log Display Preferences' with a 'Lines per Page' field set to '100'. At the bottom right, there are 'Apply', 'Save', and 'Reset' buttons.

- Use the controls to complete the configuration, as described in the following table.

Control	Description
Log Filtering	<b>Minimum Severity.</b> Select a severity level from the drop-down list. All log messages with this severity level or higher are logged.
Log Rotation	<b>Rotate every.</b> From the first drop-down list, select <b>None</b> , <b>Daily</b> , <b>Weekly</b> , or <b>Monthly</b> .
	<b>Rotate when log reaches.</b> Specify a file size in MB.
	<b>Keep at most __ log file(s).</b> Specify a number to indicate the maximum number of logs to store.
Log Display Preferences	<b>Lines per Page.</b> Specify a number to indicate the lines per page in logs.

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Remote Logging

You set remote logging in the Logging - Remote Log Servers page.

Remote logging forwards HP EFS WAN Accelerator logs to a remote server you specify.

Enabling this feature is *optional*.

### To set up remote logging

1. Click the Setup tab to display the Setup menu.
2. Click Logging to expand the Logging menu.
3. Click Remote Log Servers to display the Logging - Remote Log Servers page.

**Figure 2-53.** Logging - Remote Log Servers Page

The screenshot displays the 'Logging - Remote Log Servers' configuration page. At the top, there's a navigation bar with 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The 'Logging' tab is active, and the status is 'Healthy [config save required]'. The user is logged in as 'admin'. The left sidebar lists various configuration options, with 'Logging' expanded and 'Remote Log Servers' selected. The main content area has a title 'Logging - Remote Log Servers' and a message: 'Add any remote syslog servers you want to use for logging.' Below this is a table with two columns: 'Remote Syslog Server' and 'Min. Severity'. The table is currently empty, with the text 'No remote syslog servers.' displayed. A 'Remove Selected Servers' button is present. A modal window titled 'Add Remote Syslog Server:' is open, containing a 'Server IP' text field, a 'Minimum Severity' dropdown menu set to 'Notice', and an 'Add Server' button. At the bottom right of the main content area, there are 'Save' and 'Reset' buttons.

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add Remote Syslog Server	<b>Server IP.</b> Specify the IP address for the system log server ( <b>syslog</b> ).
	<b>Minimum Severity.</b> Select a severity level from the drop-down list.
	<b>Add Server.</b> Click <b>Add Server</b> to add the remote server to the Remote Syslog Server list.
	<b>Remove Selected Servers.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Servers</b> .

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting the Date and Time

This section describes how to set the date and time, and Network Time Protocol (NTP) servers for the HP EFS WAN Accelerator. It includes the following sections:

- ◆ “Setting the Date and Time,” next
- ◆ “Setting NTP Servers” on page 126

### Setting the Date and Time

To set the date and time

You set the date, time, and time zone in the Date & Time - Set Clock page.

1. Click the Setup tab to display the Setup menu.
2. Click Date & Time to display the Date & Time - Set Clock page.

Figure 2-54. Date & Time - Set Clock Page

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Set Time Using NTP Time Synchronization	Specify this option to enable NTP time synchronization. NTP synchronization enables the time stamps for logs to match those of other computers that use NTP time synchronization. This option is not required for proper system operation.
Set Time Manually	<b>Date.</b> Specify the current date. Use the following format: <b>YYYY/MM/DD</b> . <b>Time.</b> Specify the current time. Use the following format: <b>HH:MM:SS</b> .
Time Zone	Select your time zone from the drop-down list. The default is <b>GMT</b> (Greenwich Mean Time).

---

**NOTE:** If you change the time zone, log messages retain the old time zone until you reboot the HP EFS WAN Accelerator.

---

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting NTP Servers

You set clock synchronization using NTP in the Date & Time - NTP Servers page.

Enabling NTP time synchronization enables the time stamps on the HP EFS WAN Accelerator logs to match those of other computers using NTP time synchronization. While this option is not generally required for proper appliance operation, NTP is required if you use PFS. For detailed information, see [“Enabling Proxy File Service” on page 99](#).

### To set an NTP server

1. Click the Setup tab to display the Setup menu.
2. Click Date & Time to expand Date & Time menu.
3. Click NTP Servers to display the Date & Time - NTP Servers page.

**Figure 2-55.** Date & Time - NTP Servers Page

Home : Setup : Reports : Logging : Help    Status: **Healthy**    Logged in as: admin [logout]

### Date & Time - NTP Servers

If NTP time synchronization is enabled, please configure your remote NTP servers here.

Server	Version	Enabled
<input type="checkbox"/> 192.6.38.127	4	true
<input type="checkbox"/> 206.169.145.179	4	true
<input type="checkbox"/> 66.187.224.4	4	true
<input type="checkbox"/> 66.187.233.4	4	true

**Add New NTP Server:**  
Server IP:   
Version:   
Enabled:

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New NTP Server	<b>Server IP.</b> Specify the IP address for the NTP server.
	<b>Version.</b> Select the NTP protocol version number from the drop-down list.
	<b>Enabled.</b> Select <b>True</b> to enable synchronization; select <b>False</b> to disable.
	<b>Add Server.</b> Click <b>Add Server</b> to add the NTP server to the list.
	<b>Enable/Disable.</b> Enable or disable an NTP server.
	<b>Remove Selected Servers.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Servers</b> .

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting Authentication Methods

This section describes how to set administrator and monitor passwords, Remote Authentication Dial-In User Service (RADIUS), and Terminal Access Controller Access Control System (TACACS+) authentication. It includes the following sections:

- ◆ [“Setting General Authentication,”](#) next
- ◆ [“Setting the Administrative Password”](#) on page 129
- ◆ [“Setting the Monitor Password”](#) on page 130
- ◆ [“Setting RADIUS Servers”](#) on page 131
- ◆ [“Setting TACACS+ Servers”](#) on page 133
- ◆ [“Modifying Web Settings”](#) on page 135
- ◆ [“Setting the Message of the Day \(MOTD\)”](#) on page 136

## Setting General Authentication

You can prioritize local, RADIUS, and TACACS+ authentication methods for the system and set the authorization policy and default user for RADIUS and TACACS+ authorization systems in the Setup: Authentication - General Settings page.

**IMPORTANT:** Make sure to put the authentication methods in the order in which you want authentication to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.

**TIP:** To set TACACS+ authorization levels (**admin** or **read-only**) to allow certain members of a group to log in, add the following attribute to **users** on the TACACS+ server:

```
service = rbt-exec {
    local-user-name = "monitor"
```

}  
where you replace **monitor** with **admin** for write access.

For detailed information about setting up RADIUS and TACACS+ servers, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

## To set an authentication method

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to display the Authentication - General Settings page.

**Figure 2-56. Authentication - General Settings Page**

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Authentication Methods	<b>Method 1.</b> Select <b>Local</b> , <b>RADIUS</b> , or <b>TACACS+</b> from the drop-down list.
	<b>NOTE:</b> Make sure you put the authentication methods in the order in which you want them to occur. If authorization fails on the first method, the next method is attempted, and so forth, until all the methods have been attempted.
	<b>Method 2.</b> Select <b>None</b> , <b>Local</b> , <b>RADIUS</b> , or <b>TACACS+</b> from the drop-down list.
	<b>Method 3.</b> Select <b>None</b> , <b>Local</b> , <b>RADIUS</b> , or <b>TACACS+</b> from the drop-down list.



Control	Description
Advanced Authorization	<p><b>Authorization Policy.</b> Optionally, select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Remote-First.</b> If a local-user mapping attribute is returned and it is a valid local user name, map the authenticated user to the local user specified in the attribute. If the attribute is not present or not valid locally, use the user name specified by the default-user command. This is the default behavior.</li> <li>• <b>Remote-Only.</b> Map only to a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is attempted.</li> <li>• <b>Local-Only.</b> All remote users are mapped to the user specified. Any vendor attributes received by an authentication server are ignored.</li> </ul> <p><b>Default User.</b> Optionally, select <b>Admin</b> or <b>Monitor</b> from the drop-down list.</p>

4. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting the Administrative Password

You can change the administrator password Authentication - Account: Admin page.

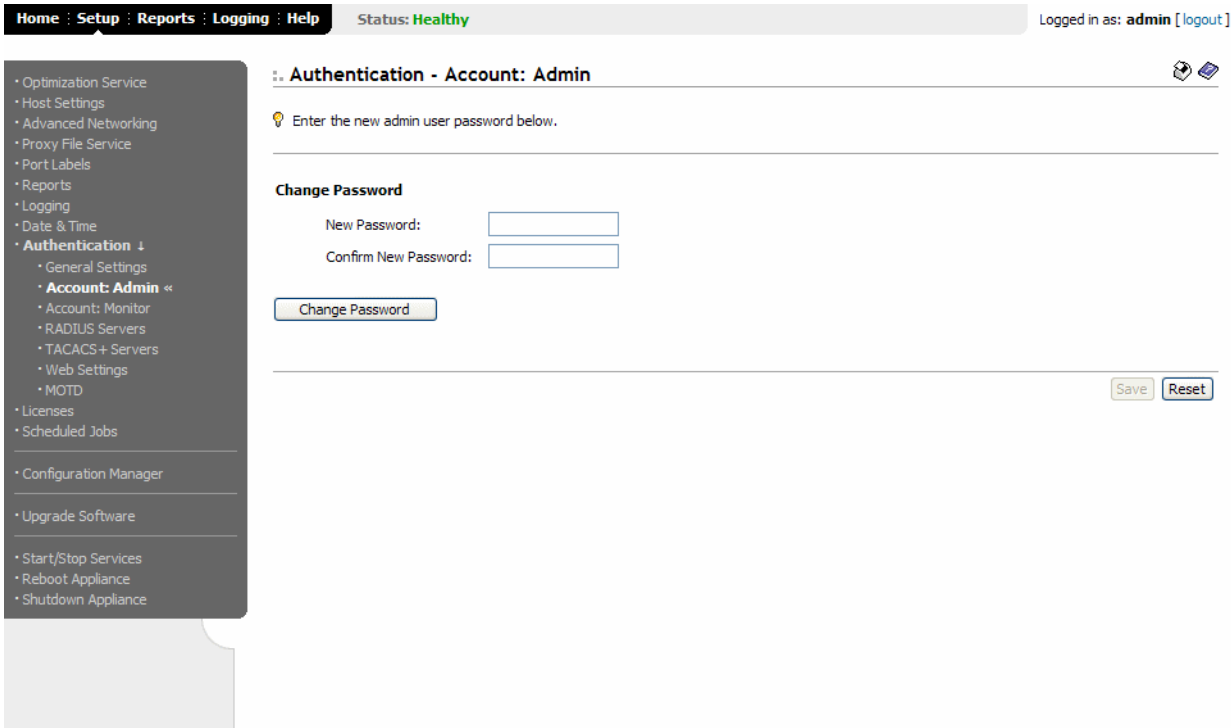
During the initial setup, you set the administrator password.

The administrator user has full privileges. For example, as an administrator you can set and modify configuration settings, restart the HP EFS WAN Accelerator service, reboot the appliance, and create and view performance and system reports.

To set the administrator password

- 1. Click the Setup tab to display the Setup menu.
- 2. Click Authentication to expand the Authentication menu.
- 3. Click Account: Admin to display the Authentication - Account: Admin page.

Figure 2-57. Authentication - Account: Admin Page



- 4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Change Password	<b>New Password.</b> Specify the new administrator password. The password must have a minimum of 6 characters.
	<b>Confirm New Password.</b> Retype the new administrator password.
	<b>Change Password.</b> Click <b>Change Password</b> to apply your changes.

- 5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

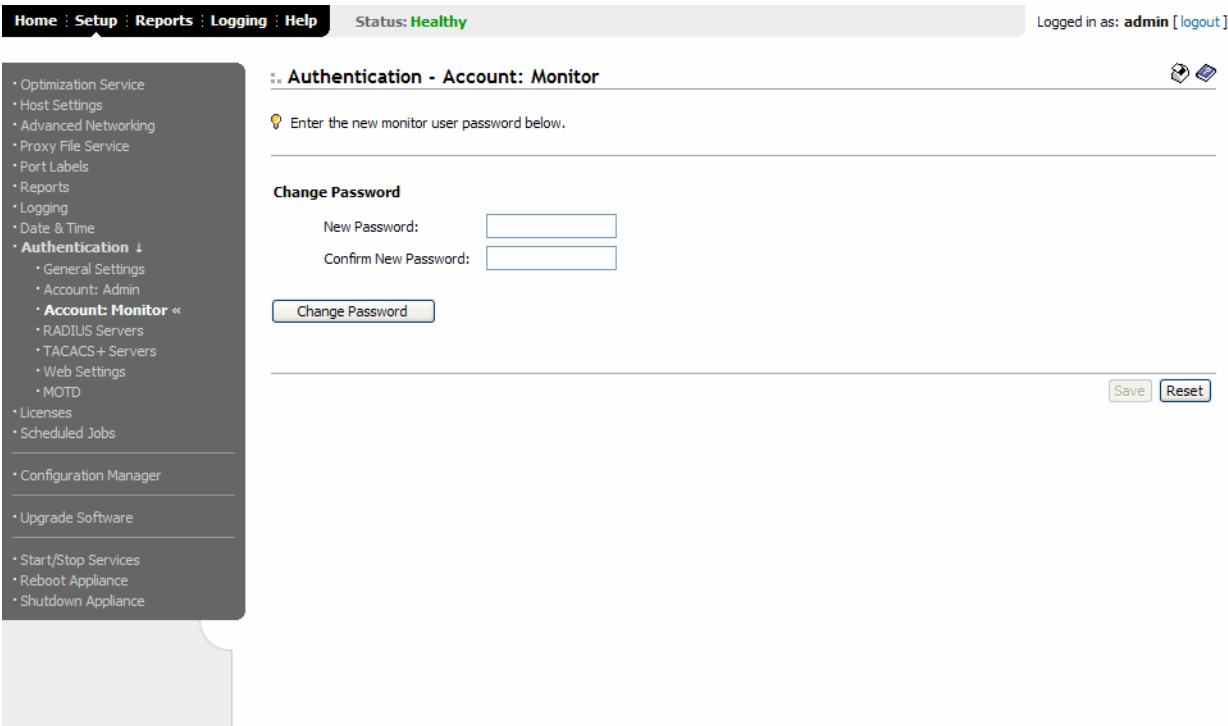
Setting the Monitor Password

You set the monitor user password in the Authentication - Account: Monitor page.  
A monitor user can view reports; a monitor user cannot make configuration changes.

### To set the monitor password

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to expand the Authentication menu.
3. Click Account: Monitor to display the Authentication - Account: Monitor page.

Figure 2-58. Authentication - Account: Monitor Page



4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Change Password	<b>New Password.</b> Specify the new administrator password. The password must have a minimum of 6 characters.
	<b>Confirm New Password.</b> Retype the new administrator password.
	<b>Change Password.</b> Click <b>Change Password</b> to apply your changes.

5. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

### Setting RADIUS Servers

You set up RADIUS server authentication in the Authentication - RADIUS Servers page.

RADIUS is an access control protocol that uses a challenge and response method for authenticating users. Setting up RADIUS server authentication is optional.

For detailed information about setting up RADIUS and TACACS+ servers, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

Enabling this feature is *optional*.

## To set RADIUS server authentication

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to expand the Authentication menu.
3. Click RADIUS Servers to display the Authentication - RADIUS Servers page.

**Figure 2-59. Authentication - RADIUS Servers Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: **admin** [ logout ]

**Authentication - RADIUS Servers**

Configure your RADIUS authentication settings.  
This configuration is only necessary for appliances using RADIUS authentication.

**General**

Server Key:

Timeout:  seconds (1-60)

Retries:  (0-5)

Green indicates use of a global value

Server IP	Port	Key	Timeout	Retries	Enabled
No RADIUS servers.					

**Add New RADIUS Server:**

Server IP:

Authentication Port:

Server Key:

Timeout:  seconds (1-60)

Retries:  (0-5)

Enabled:

4. Use controls to complete the configuration, as described in the following table.

Control	Description
General	<b>Server Key.</b> Specify the server key.
	<b>Timeout.</b> Specify the time-out period.
	<b>Retries.</b> Specify the number of times you want to allow the user to retry authentication.
	<b>Apply.</b> Click <b>Apply</b> to apply your settings to the running configuration.

Control	Description
Add New RADIUS Server	<b>Server IP.</b> Specify the server IP address.
	<b>Authentication Port.</b> Specify the port for the server.
	<b>Server Key.</b> Specify the server key.
	<b>Timeout.</b> Specify the time-out period.
	<b>Retries.</b> Specify the number of times you want to allow the user to retry authentication. Valid values are <b>0-5</b> .
	<b>Enabled.</b> Select <b>True</b> to enable; select <b>False</b> to disable.
	<b>Add Server.</b> Click <b>Add Server</b> to add the RADIUS server to the list.
Enable/Disable	Enable or disable a RADIUS server.
Remove Selected Servers	<b>Remove Selected Servers.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Servers</b> .

---

**NOTE:** If you add a new server to your network and you do not specify these fields at that time, the global settings are applied automatically.

---

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting TACACS+ Servers

You set up TACACS+ server authentication in the Authentication - TACACS+ Servers page.

Enabling this feature is *optional*.

TACACS+ is an authentication protocol that allows a remote access server to forward a login password for a user to an authentication server to determine whether access is allowed to a given system.

For detailed information about configuring RADIUS and TACACS+ servers to accept login requests from the HP EFS WAN Accelerator, see the *HP StorageWorks Enterprise File Services WAN Accelerator Deployment Guide*.

## To set a TACACS+ server

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to expand the Authentication menu.
3. Click TACACS+ Servers to display the Authentication - TACACS+ Servers page.

**Figure 2-60. Authentication - TACACS+ Servers Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: **admin** [ logout ]

**Authentication - TACACS+ Servers**

Configure your TACACS+ authentication settings.  
This configuration is only necessary for appliances using TACACS+ authentication.

**General**

Server Key:

Timeout:  seconds (1-60)

Retries:  (0-5)

[Apply](#)

Green indicates use of a global value

Server IP	Port	Type	Key	Time-Out	Retries	Enabled
No TACACS+ servers.						

[Remove Selected Servers](#)    [Enable](#)    [Disable](#)

**Add New TACACS+ Server:**

Server IP:

Authentication Port:

Authentication Type:

Server Key:

Timeout:  seconds (1-60)

Retries:  (0-5)

Enabled:

[Add Server](#)

[Save](#)    [Reset](#)

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
General	<b>Server Key.</b> Specify the server key.
	<b>Timeout.</b> Specify the time-out period.
	<b>Retries.</b> Specify the number of times you want to allow the user to retry authentication.
	<b>Update Settings.</b> Click <b>Update Settings</b> to update your global TACACS+ settings.

Control	Description
Add New TACACS+ Server	<b>Server IP.</b> Specify the server IP address.
	<b>Authentication Port.</b> Specify the port for the server.
	<b>Authentication Type.</b> Select <b>ASCII</b> or <b>PAP</b> from the drop-down list.
	<b>Server Key.</b> Specify the server key.
	<b>Timeout.</b> Specify the time-out period.
	<b>Retries.</b> Specify the number of times you want to allow the user to retry authentication. Valid values are <b>0-5</b> .
	<b>Enabled.</b> Select <b>True</b> to enable; select <b>False</b> to disable.
	<b>Add Server.</b> Click <b>Add Server</b> to add the TACACS+ server to the list.
Enable/Disable	Enable or disable a TACACS+ server.
Remove Selected Servers	<b>Remove Selected Servers.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Servers</b> .

---

**NOTE:** If you add a new server to your network and you do not specify these fields at that time, the global settings are applied automatically.

---

- Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Modifying Web Settings

You can modify Management Console Web user interface settings in the Authentication: Web Settings page.

## To modify Web settings

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to expand the Authentication menu.
3. Click Web Settings to display the Authentication - Web Settings page.

**Figure 2-61. Authentication: Web Settings Page**

The screenshot shows the 'Authentication - Web Settings' page. The top navigation bar includes 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy' and the user is logged in as 'admin'. The sidebar on the left lists various configuration options, with 'Authentication' expanded to show 'Web Settings'. The main content area has a title 'Authentication - Web Settings' and a subtitle 'Check and modify your web authentication settings.' Below this, there are two sections: 'Login Page' with a 'Default Login ID' field set to 'admin', and 'Timeout' with a 'Web Inactivity Time-Out' field set to '15' minutes. At the bottom right, there are three buttons: 'Apply', 'Save', and 'Reset'.

4. Use the controls to complete the configuration, as described in the following table.

Control	Description
Login Page	<b>Default Login ID.</b> If desired, modify the user name that appears by default on the authentication page. The default is <b>admin</b> .
Timeout	<b>Web Activity Time-Out.</b> Specify the number of idle minutes before time-out. Specify <b>0</b> to disable time-out.

5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Setting the Message of the Day (MOTD)

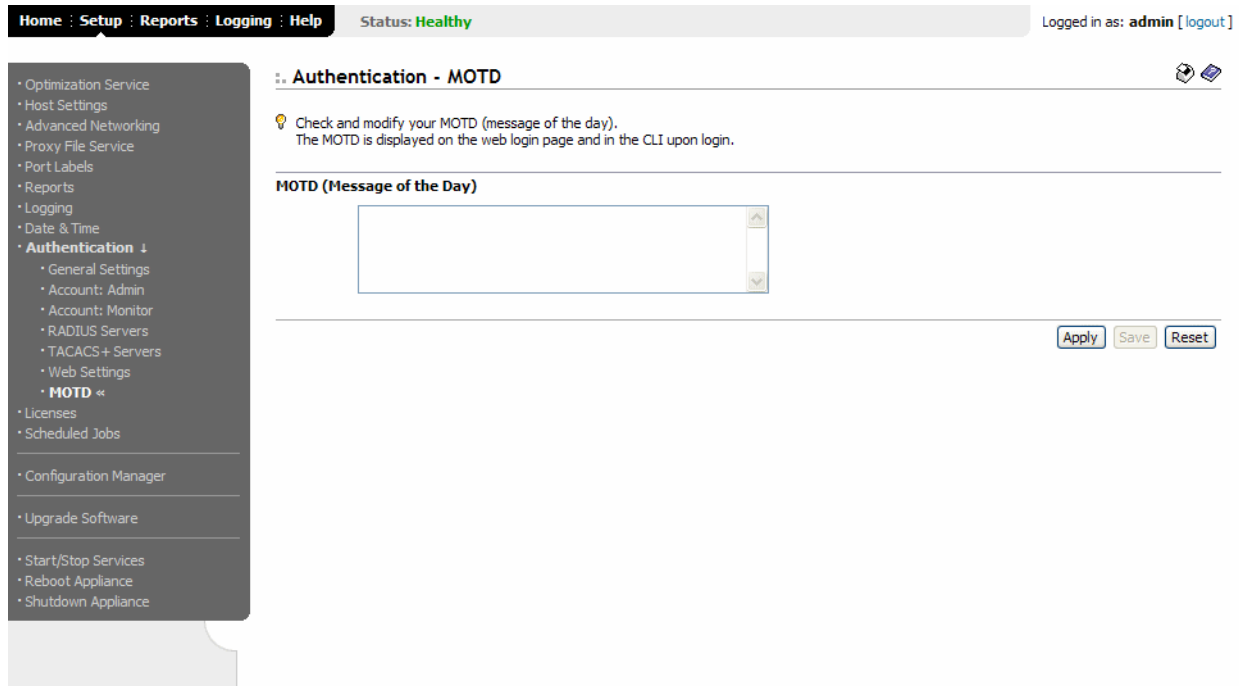
You can create or modify a message of the day that appears in the Management Console or in the CLI in the Authentication - MOTD page.



## To set a MOTD

1. Click the Setup tab to display the Setup menu.
2. Click Authentication to expand the Authentication menu.
3. Click MOTD in to display the Authentication - MOTD page.

Figure 2-62. Authentication - MOTD Page



4. Type a message in the **MOTD (Message of the Day)** text box.
5. Click **Apply** to apply your settings to the running configuration. (Apply your settings to test a new configuration before saving them permanently.)
6. Click **Save** to save your settings permanently or click **Reset** to return the settings to their previous values.

## Managing Licenses

This section describes how to manage HP EFS WAN Accelerator licenses.

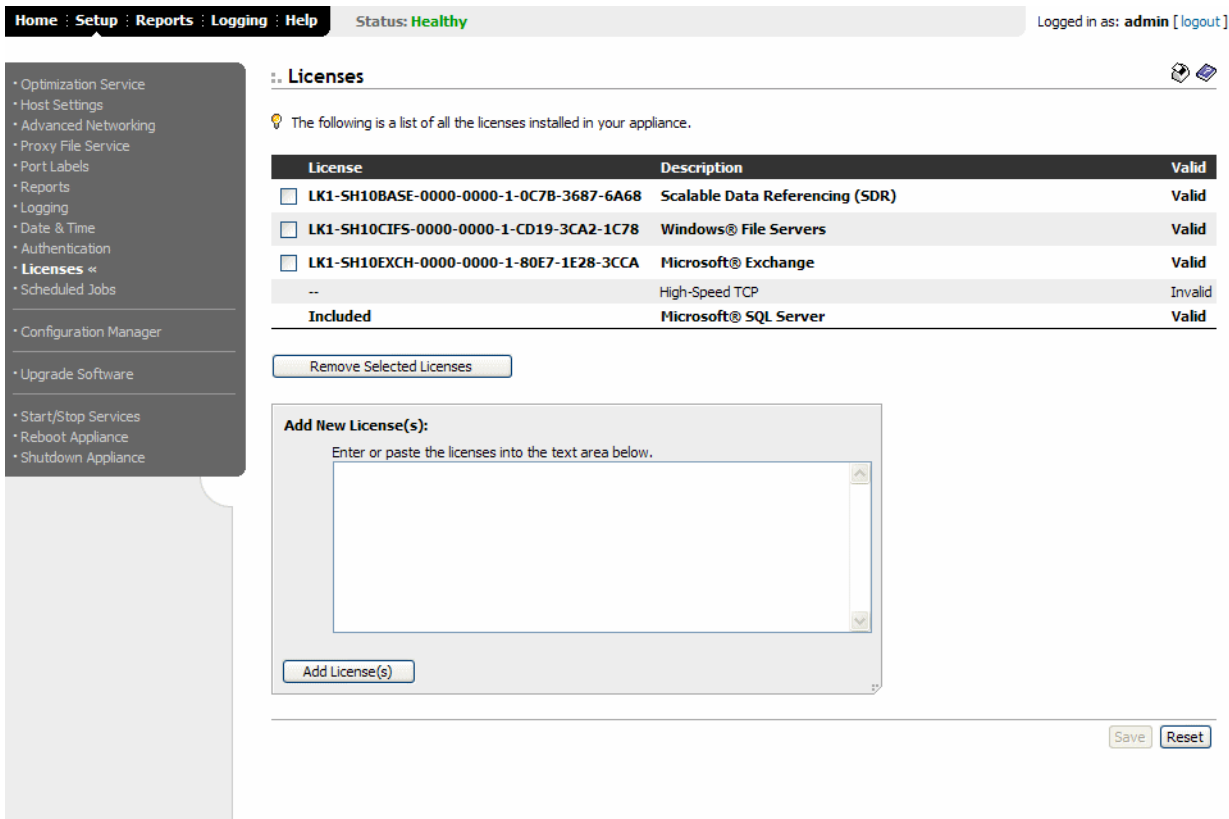
### Updating Your Licenses

You can view a list of active licenses, update expired licenses, and add new license keys in the Licenses page.

To update a license

- 1. Click the Setup tab to display the Setup menu.
- 2. Click Licenses to display the Licenses page.

Figure 2-63. Licenses Page



- 3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Add New License	<b>Add License.</b> Copy and paste the license key provided by HP into the <b>Add New License(s)</b> text box, and click <b>Add License</b> to add a license.
	<b>TIP:</b> Separate multiple license keys with a space, tab, or ENTER.
	<b>Remove Selected Licenses.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Licenses</b> .

- 4. Click **Save** to write the new license to disk or click **Reset** to return the settings to their previous values.

Viewing Scheduled Jobs

This section describes how to view scheduled jobs.

## Viewing Scheduled Jobs

You can view completed, pending, inactive jobs, as well as jobs that were not completed because of an error in the Scheduled Jobs page.

Jobs are CLI commands that are scheduled to execute at a time you specify.

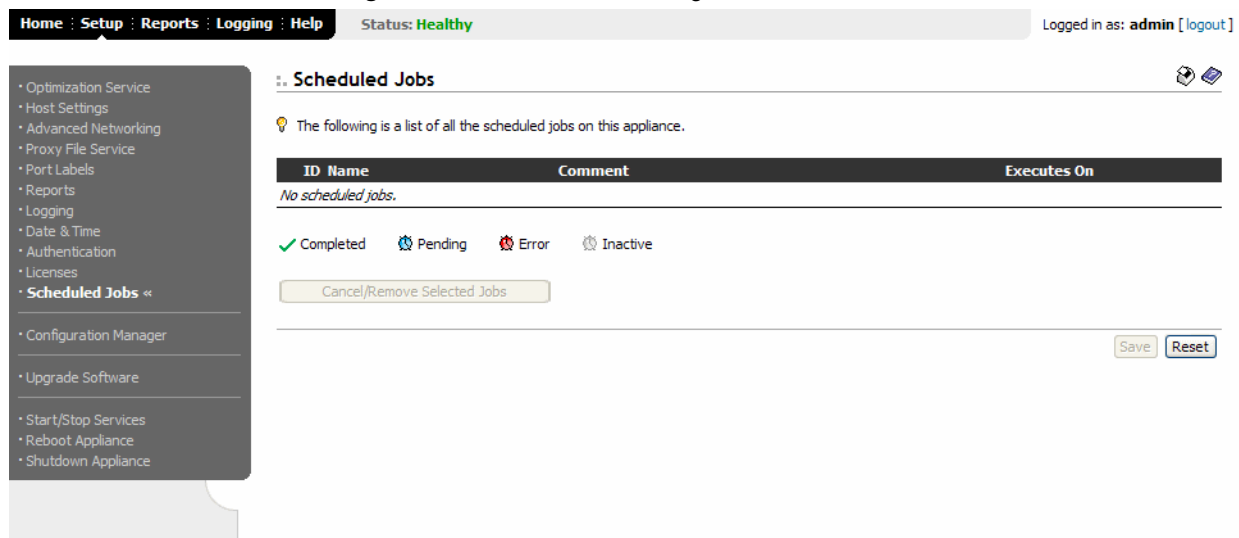
The only job you can schedule using the Management Console are software upgrades; for all other jobs, you must use the CLI.

For detailed information about scheduling jobs using the CLI, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command Line-Interface Reference Manual*.

### To view scheduled jobs

1. Click the Setup tab to display the Setup menu.
2. Click Scheduled Jobs to display the Scheduled Jobs page.

**Figure 2-64.** Scheduled Jobs Page



3. To remove an entry, click the check box next to the name and click **Cancel/Remove Selected Jobs**.
4. Click **Save** to save your settings permanently or click **Reset** to return your settings to their previous values.

## Managing Configurations

You can save, activate, and import configurations in the Configuration Manager Page.

Each HP EFS WAN Accelerator has an active, running configuration and written, saved configurations.

When you **Apply** your settings in the Management Console, the values are applied to the active running configuration, but the values are not written to disk and saved permanently.

When you **Save** your configuration settings, the values are written to disk and saved permanently. They take effect after you restart the HP EFS WAN Accelerator service.

Each time you save your configuration settings, they are written to the current running configuration, and a backup is created. For example, if the running configuration is **myconfig** and you save it, **myconfig** is backed up to **myconfig.bak** and **myconfig** is overwritten with the current configuration settings.

The Configuration Manager is a utility that enables you to save configurations as backups or active configuration backups.

The Configuration Manager also includes an Import Configuration utility to support these common use cases:

- ◆ **Replacing an HP EFS WAN Accelerator.** If you are swapping one HP EFS WAN Accelerator for another, you can import all of the network information (although not the licenses) and disconnect the old HP EFS WAN Accelerator before you switch configurations on the new HP EFS WAN Accelerator.
- ◆ **Configuration template for a large deployment.** You can avoid entering the complete HP EFS WAN Accelerator configuration for each of many appliances by setting up a template HP EFS WAN Accelerator and importing template settings to the configuration list.

---

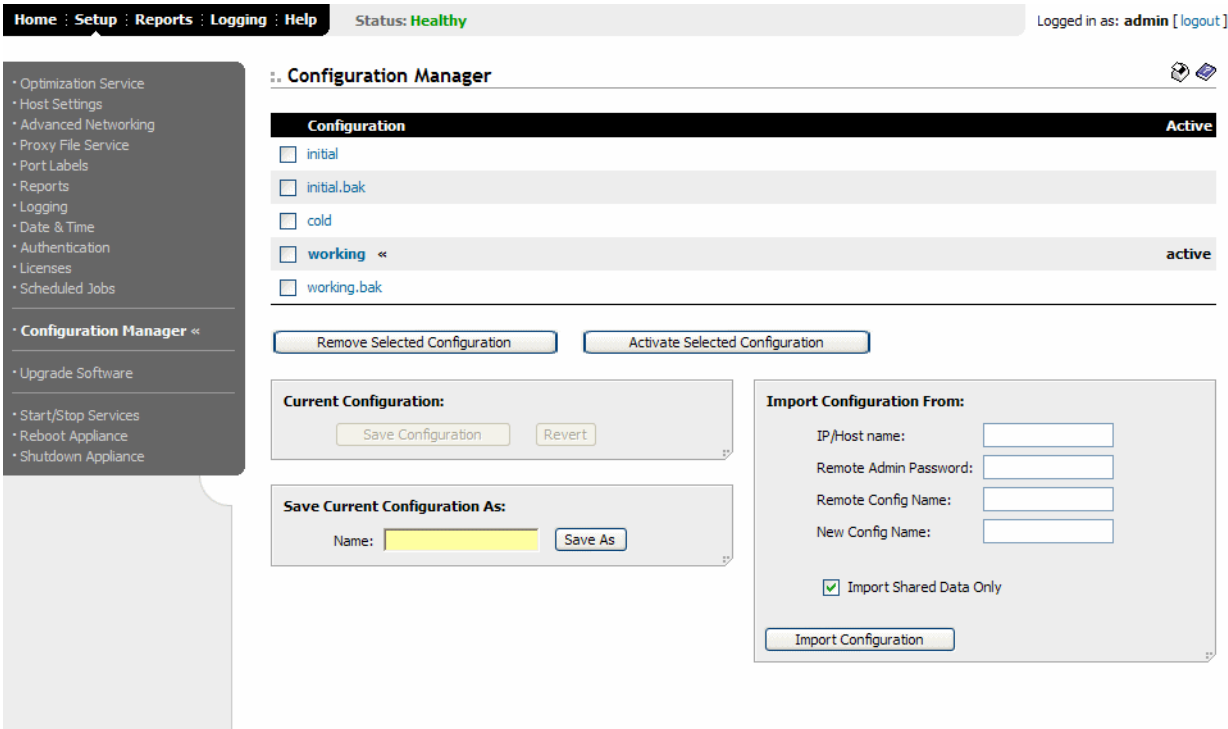
**IMPORTANT:** Some configuration settings require you to restart the HP EFS WAN Accelerator service for the settings to take effect. For detailed information about restarting the HP EFS WAN Accelerator service, see [“Starting and Stopping Services” on page 144](#).

---

# To manage configurations

1. Click the Setup tab to display the Setup menu.
2. Click Configuration Manager to display Configuration Manager page.

Figure 2-65. Configuration Manager Page



3. Use the controls to manage configurations, as described in the following table.

Control	Description
Current Configuration	<b>Save Configuration.</b> To save settings that have been applied to the running configuration, click <b>Save Configuration</b> .
	<b>Revert.</b> To revert your settings to the running configuration, click <b>Revert</b> .
	<b>Save Current Configuration As.</b> To save settings that have been applied to the running configuration as a new file, type a name in the <b>Name</b> text box and click <b>Save As</b> . The configuration name you specify does not become the active configuration.
	<b>Activate Selected Configuration.</b> To activate an alternative configuration, click the check box next to the entry and click <b>Activate Selected Configuration</b> .
	<b>Remove Selected Configuration.</b> To remove an entry, click the check box next to the entry and click <b>Remove Selected Configuration</b> .

Import Configuration From	<p><b>IP/Host Name.</b> Specify the IP address or host name of the HP EFS WAN Accelerator from which you want to import the configuration.</p> <p><b>Remote Admin Password.</b> Specify the administrator password for the remote HP EFS WAN Accelerator.</p> <p><b>Remote Config Name.</b> Specify the name of the configuration you want to import from the remote HP EFS WAN Accelerator.</p> <p><b>New Config Name.</b> Specify a new, local, configuration name for this appliance.</p> <p><b>Import Shared Data Only.</b> This is enabled by default. Keep this option checked to copy only the following common settings: in-path and out-of-path interface, protocols, CLI and Web, statistics, NTP, SNMP, and alarm settings. The following settings are not automatically copied: failover, SNMP (contact and location), log, and network settings.</p> <p><b>Import Configuration.</b> To perform the import configuration operation, click <b>Import Configuration</b>.</p> <p>The imported configuration appears in the Configuration list but does not become the active configuration until you click <b>Activate</b>.</p>
	<p><b>TIP:</b> Click the configuration name to display the configuration settings in a new browser window.</p>
	<p><b>IMPORTANT:</b> You must restart the HP EFS WAN Accelerator service for a configuration to take effect. For detailed information, see <a href="#">“Starting and Stopping Services” on page 144</a>.</p>

## Upgrading Your Software

You can upgrade or revert to a back-up version of the software in the Software Upgrade page.

## To upgrade or revert software versions

1. Click the Setup tab to display the Setup menu.
2. Click Upgrade Software to display the Software Upgrade page.

Figure 2-66. Software Upgrade Page

3. Use the controls to complete the configuration, as described in the following table.

Control	Description
Install Upgrade From	<p><b>URL.</b> Specify this option and type the URL.</p> <p>If you specify a URL in the URL text box, the image is uploaded, installed, and the HP EFS WAN Accelerator is rebooted at the time you specify.</p> <p><b>Local File.</b> Specify this option and type the path or click <b>Browse</b> to navigate to the local file directory.</p> <p>If you specify a file to upload in the <b>Local File</b> text box, the image is uploaded immediately, however the image is installed and the HP EFS WAN Accelerator is rebooted at the time you specify.</p> <p><b>Install Upgrade.</b> Click <b>Install Image</b> to install the new version of the software.</p> <p><b>Schedule Upgrade for Later.</b> Specify this option to schedule the upgrade process. Specify the date and time for the upgrade:</p> <ul style="list-style-type: none"> <li>• <b>Date.</b> Specify the date to run the operation, following the format <b>YYYY/MM/DD</b>.</li> <li>• <b>Time.</b> Specify the time to run the operation, following the format <b>HH:MM:SS</b>.</li> </ul>
Switch to Backup Version	To revert to the previous software version (identified on this page), click <b>Switch to Backup Version</b> . The process starts immediately.

**IMPORTANT:** You must restart the HP EFS WAN Accelerator service for this configuration to take effect. For detailed information, see “Starting and Stopping Services” on page 144.

---

## Starting and Stopping Services

You can start, stop, and restart the HP EFS WAN Accelerator service in the Start/Stop Services page.

The HP EFS WAN Accelerator service is a daemon that execute in the background, performing operations when required.

Many of the HP EFS WAN Accelerator service commands are initiated at startup. It is important to restart the HP EFS WAN Accelerator service when you have made changes to your configuration.

---

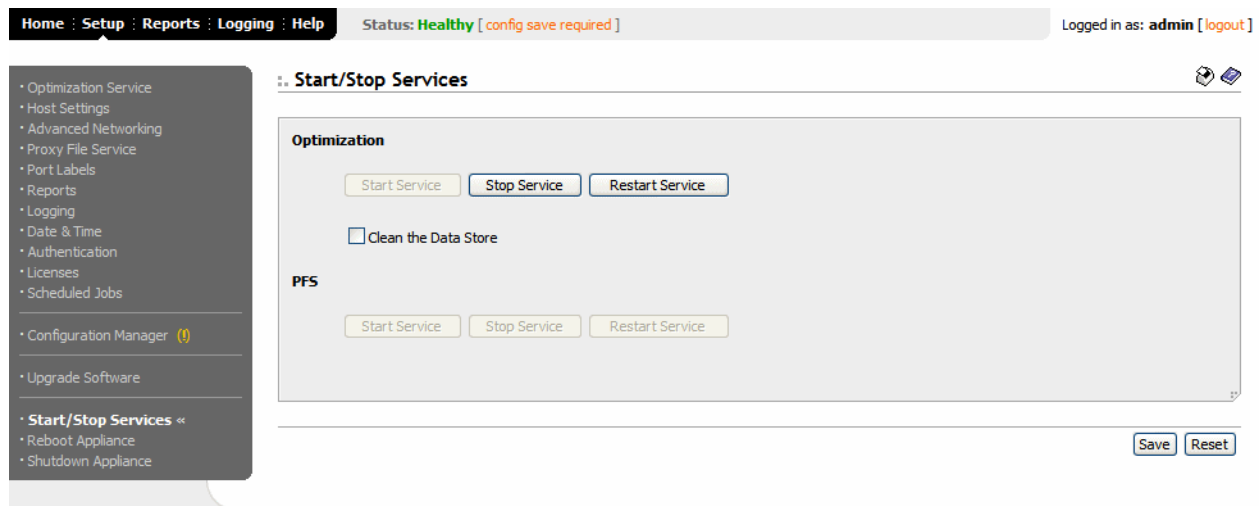
**WARNING:** Restarting the HP EFS WAN Accelerator service disrupts existing network connections that are proxied through the HP EFS WAN Accelerator.

---

### To start, stop, or restart services

1. Click the Setup tab to display the Setup menu.
2. Click Start/Stop Services to display the Start/Stop Services page.

**Figure 2-67.** Start/Stop Services Page



3. Under Optimization, to start, stop, or restart the HP EFS WAN Accelerator service, click the appropriate button.
4. Click **Save** to save your settings permanently or click **Reset** to return your settings to their previous values.

---

**TIP:** To remove data from the data store, click **Clean the Data Store**. (You rarely need to clean the data store outside of a lab environment.)

---



## Rebooting the HP EFS WAN Accelerator

You can reboot the HP EFS WAN Accelerator in the Reboot Appliance page.

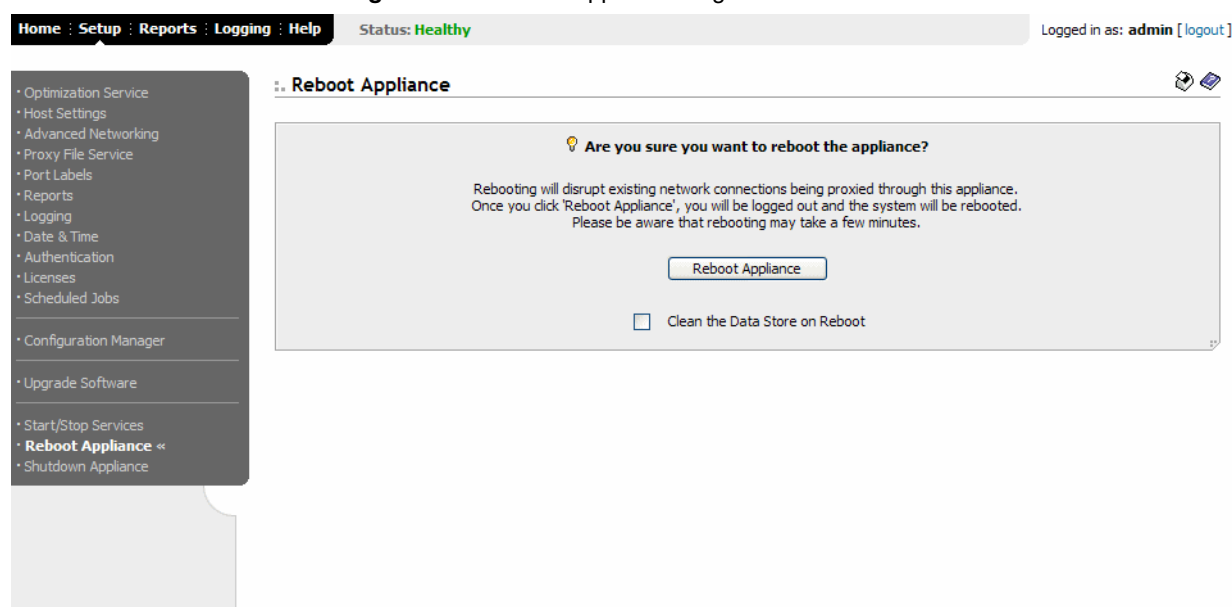
Rebooting the HP EFS WAN Accelerator disrupts existing network connections that are currently proxied through the HP EFS WAN Accelerator.

Rebooting can take a few minutes.

### To reboot the HP EFS WAN Accelerator

1. Click the Setup tab to display the Setup menu.
2. Click Reboot Appliance to display the Reboot Appliance page.

Figure 2-68. Reboot Appliance Page



3. Click **Reboot Appliance**. After you click **Reboot Appliance**, you are logged out of the system and it is rebooted

**TIP:** To remove data from the data store, click the **Clean the Data Store on Reboot** check box. (You rarely need to clean the data store outside of a lab environment.)

## Shutting Down the HP EFS WAN Accelerator

You can shut down the HP EFS WAN Accelerator in the Shutdown Appliance page.

When you shutdown the HP EFS WAN Accelerator, connections are broken and optimization ceases.

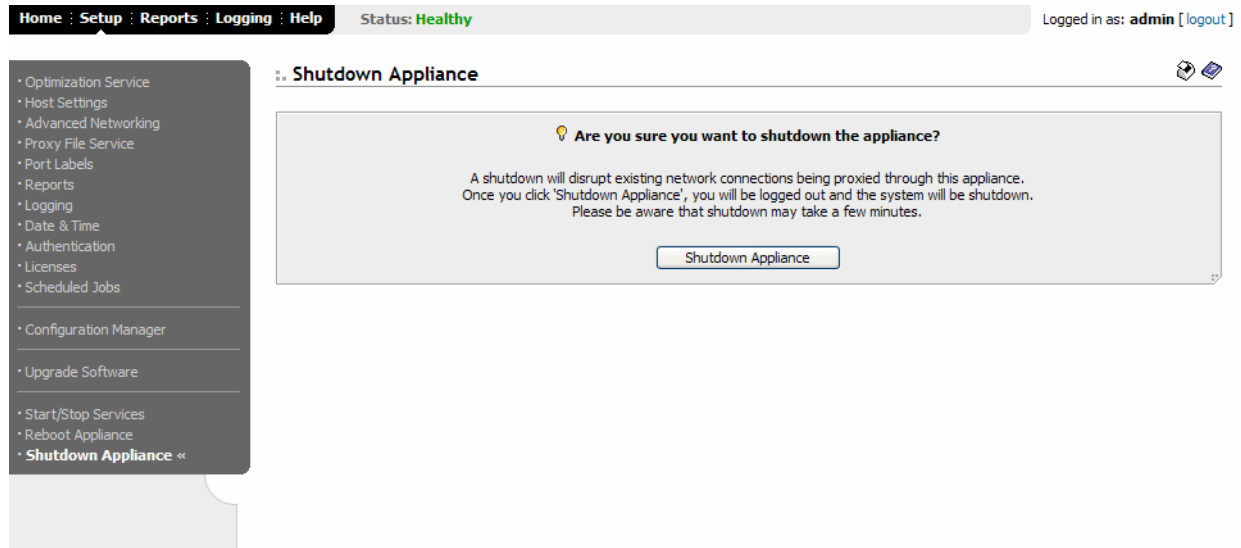
Shutdown can take a few minutes.

To restart the system, you must manually turn on the HP EFS WAN Accelerator.

## To shutdown the HP EFS WAN Accelerator

1. Click the Setup tab to display the Setup menu.
2. Click Shutdown Appliance to display the Shutdown Appliance page.

**Figure 2-69.** Shutdown Appliance Page



3. Click **Shutdown Appliance**. After you click **Shutdown Appliance**, the system is turned off. To restart the system you must manually turn on the HP EFS WAN Accelerator.

## CHAPTER 3

# Creating HP EFS WAN Accelerator Reports and Logs

## In This Chapter

This chapter describes how to create and view performance, network, health, Proxy File Service (PFS), export, and diagnostic reports. It also describes how to view HP EFS WAN Accelerator logs, contact technical support, and the online help table of contents. This chapter includes the following sections:

- ◆ [“Creating Performance Reports,” next](#)
- ◆ [“Viewing Networking Reports” on page 165](#)
- ◆ [“Viewing System Health Reports” on page 185](#)
- ◆ [“Viewing Proxy File Service Reports” on page 192](#)
- ◆ [“Exporting Performance Statistics Reports” on page 196](#)
- ◆ [“Viewing System Diagnostic Files” on page 197](#)
- ◆ [“Viewing HP EFS WAN Accelerator Logs” on page 201](#)
- ◆ [“Getting Help” on page 202](#)

---

## Creating Performance Reports

The following section describes how to create and view performance reports. It includes the following sections:

- ◆ [“Creating Bandwidth Optimization Reports,” next](#)
- ◆ [“Creating Data Store Hits Reports” on page 150](#)
- ◆ [“Creating Data Reduction Reports” on page 152](#)
- ◆ [“Creating NFS Statistics Report” on page 155](#)
- ◆ [“Creating Throughput Reports” on page 157](#)
- ◆ [“Creating Traffic Summary Reports” on page 159](#)

## Creating Bandwidth Optimization Reports

The Performance - Bandwidth Optimization report summarizes the overall inbound and outbound bandwidth improvements for your network using the HP EFS WAN Accelerator. You can create reports according to the time period of your choice, application, and type of traffic.

The Performance - Bandwidth Optimization report includes the following table of statistics that describe bandwidth activity for the time period you specify.

Field	Description
WAN Data	Specifies the bytes sent over the Wide Area Network (WAN) using the HP EFS WAN Accelerator.
LAN Data	Specifies the bytes sent over the Local Area Network (LAN) using the HP EFS WAN Accelerator.
Total Data Reduction % over Last Week	Specifies the total decrease of data transmitted over the WAN, according to the following calculation: $(\text{Data In} - \text{Data Out}) / (\text{Data In})$
Peak Data Reduction % over Last Week	Specifies the peak decrease in data transmitted over the WAN.
Peak Data Reduction Occurred At	Specifies the time that the peak data reduction occurred.
Capacity Increase	Specifies the increase in the amount of data transmitted over the WAN, according to the following calculation: $1 / (1 - \text{Reduction Rate})$

### What this Report Tells You

The Performance - Bandwidth Optimization report answers the following questions:

- ◆ How much bandwidth optimization has occurred?
- ◆ What was the average and peak amount of data sent?
- ◆ What was the rate at which data was sent?
- ◆ What was the overall increase in the amount of data that can be transmitted using the HP EFS WAN Accelerator?

### About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

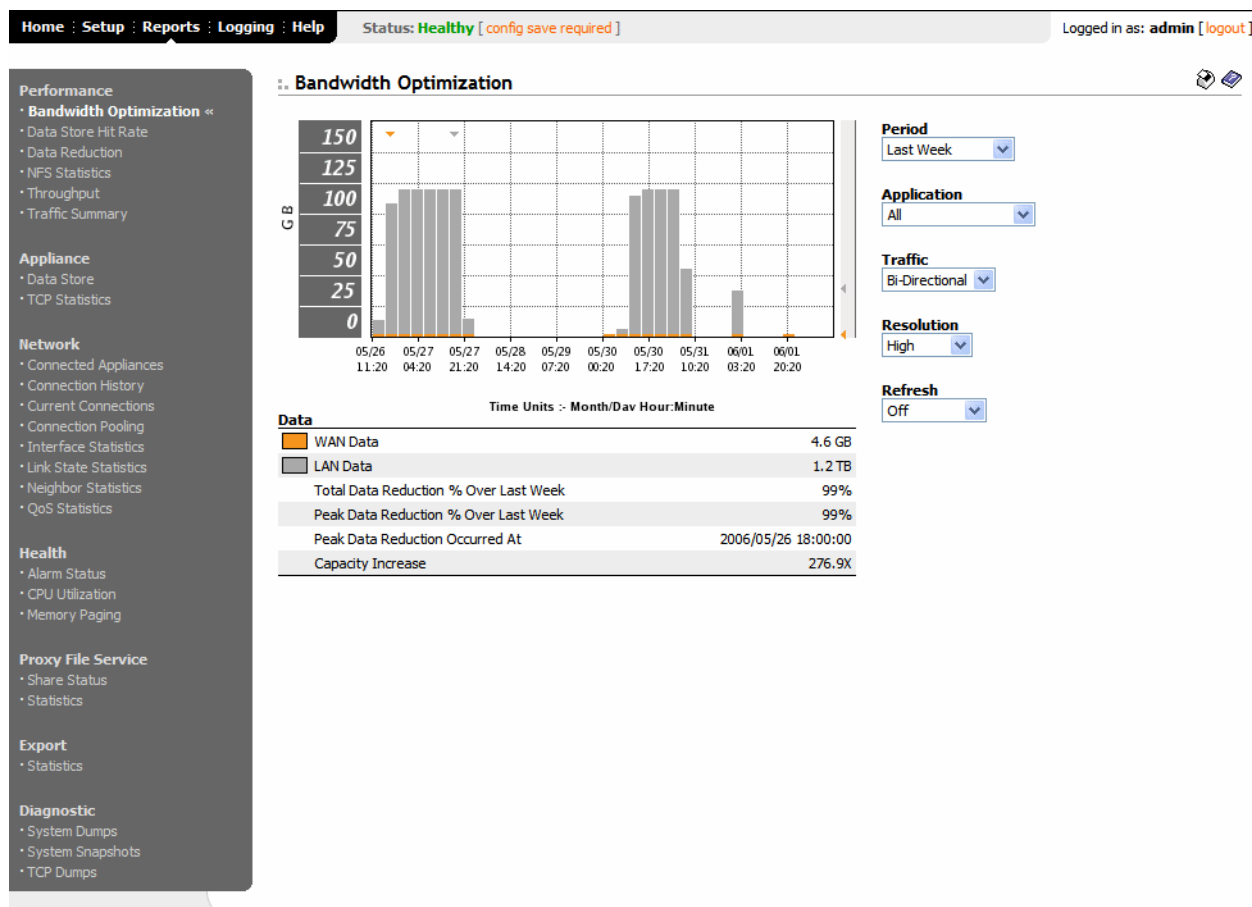
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

### To create a Bandwidth Optimization report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.

**Figure 3-1. Performance - Bandwidth Optimization Page**



2. Use the controls to customize the report, as described in the following table.

Control	Description
Period	Select <b>Last Minute</b> , <b>Last 5 Minutes</b> , <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , <b>Last Month</b> , or <b>Custom Interval</b> from the drop-down list.
Application	Select <b>FTP</b> , <b>HTTP</b> , <b>CIFS:NetBIOS</b> , <b>CIFS:TCP</b> , or <b>MAPI</b> from the drop-down list. The default value is <b>All</b> .
Traffic	Select <b>Bi-directional</b> , <b>WAN-to-LAN</b> , or <b>LAN-to-WAN</b> from the drop-down list.
Appliances	The default is to include all appliances. To set a custom group, click <b>All</b> and use the dialog box to select an HP EFS WAN Accelerator, a group, or a custom selection of HP EFS WAN Accelerators to include in the report.
Resolution	Select <b>High</b> , <b>Medium</b> , or <b>Low</b> from the <b>Resolution</b> drop-down list. <b>High</b> (small bars) allows you to drill down to specific points in time, while <b>Low</b> (large bars) enables you to count or compare aggregate values in the time interval.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15s</b>.</li><li>• To refresh your report every 30 seconds, click <b>30s</b>.</li><li>• To turn off refresh, click <b>off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating Data Store Hits Reports

The Performance - Data Store Hits report summarizes how many times the HP EFS WAN Accelerator data-store disk and memory have seen a data segment. A hit is a data segment that has been seen before by the data store in the HP EFS WAN Accelerator. If a hit has occurred, the HP EFS WAN Accelerator sends the reference to the data segment rather than the actual data over the WAN.

The Performance - Data Store Hits report contains the following table of statistics that summarize data store activity.

Field	Description
Total Hits over Last Week	Specifies the total number of hits against the data store. A hit is a data segment that has been seen before by the data store in the HP EFS WAN Accelerator. If a hit has occurred, the HP EFS WAN Accelerator sends the reference to the data rather than the actual data over the WAN.
Misses	Specifies the number of misses that occurred. A miss is an unmatched data segment—the data store has not seen the data segment before and must send all the data across the WAN. The data is Lempel-Ziv (LZ) compressed if LZ compression is enabled. For detailed information about setting optimization policies, see <a href="#">“Setting In-Path Rules” on page 25</a> .

## What This Report Tells You

The Performance - Data Store Hit Rate report answers the following questions:

- ◆ How much optimization is occurring?

- ◆ How much optimization occurred through disk hits?
- ◆ How much optimization occurred through memory hits?
- ◆ How much data traversed the WAN without optimization?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

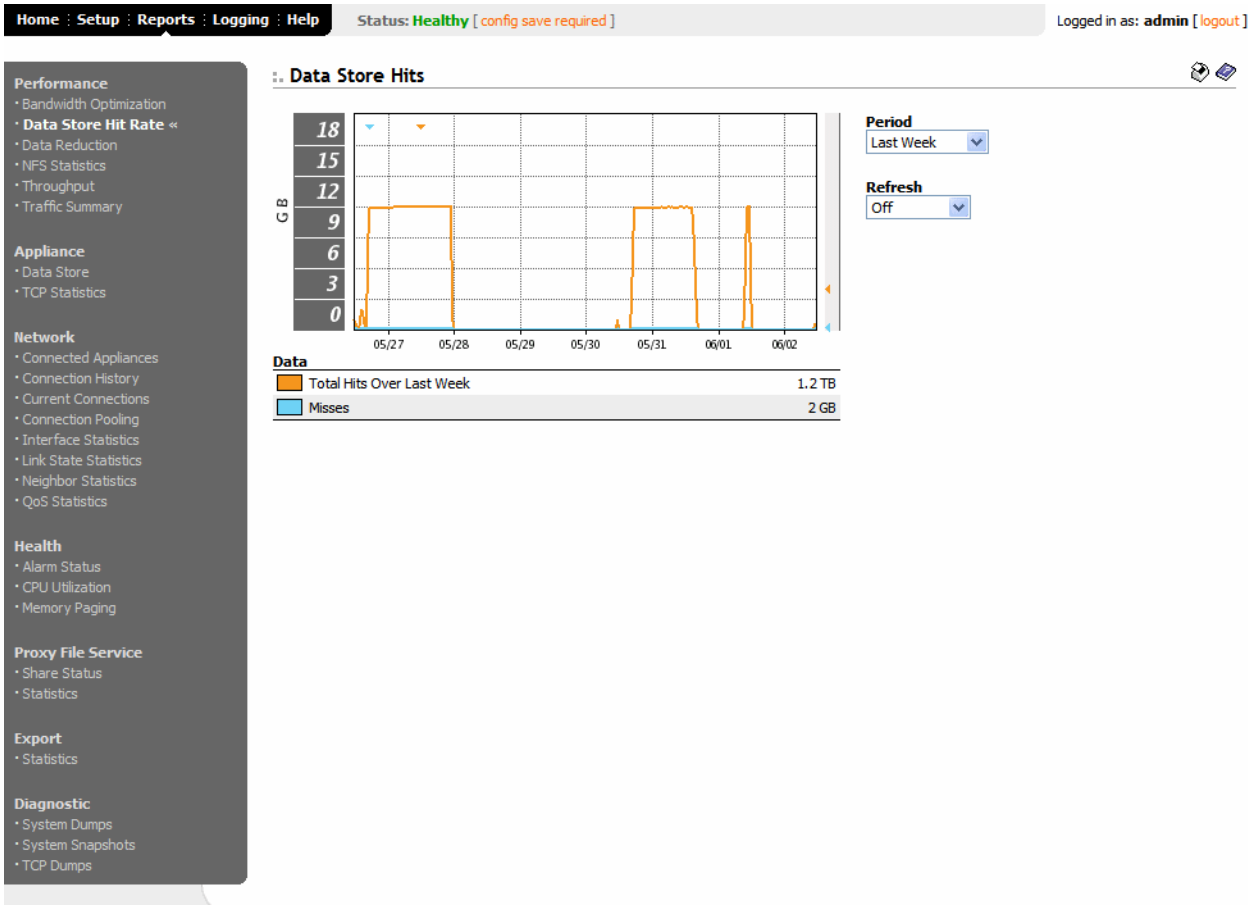
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the Data Store Hits report

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Performance in the left menu, click Data Store Hit Rate to display the Performance - Data Store Hits page.

Figure 3-2. Performance - Data Store Hit Rate Page



- 3. Select **Last 5 Minutes**, **Last Hour**, **Last Day**, **Last Week**, or **Last Month** from the drop-down list.

**TIP:** To refresh your report every 15 seconds, click **15s**. To refresh your report every 30 seconds, click **30s**.

**TIP:** To print your report, click the **Printer** icon in the upper right corner of the page.

Creating Data Reduction Reports

The Performance - Data Reduction report summarizes the percent reduction of data transmitted by an application such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), NetBIOS and Transmission Control Protocol (TCP), traffic in Common Internet File Systems (CIFS), and Messaging Application Protocol Interface (MAPI).



The Performance - Data Reduction report includes the following table of statistics that describe data reduction for the application and the time period you specify.

Field	Description
Total Data Reduction % Over Last Week	Specifies the total decrease of data transmitted over the WAN.
Peak Data Reduction % Over Last Week	Specifies the peak decrease in data transmitted over the WAN.
Peak Data Reduction Occured At	Specifies the time that the peak data reduction occurred.
Capacity Increase	Specifies the increase in the amount of the data that can be transmitted over the WAN.

## What This Report Tells You

The Performance - Data Reduction report answers the following questions:

- ◆ What was the total reduction in the amount of data that can be transmitted for each application?
- ◆ What was the peak reduction in the amount of data transmitted for each application?
- ◆ What was the total capacity increase for the application and time period specified?

## About Report Graphs

In bar-graph and line-graph reports, the *x*-axis (or tick mark) plots time, according to the interval you select. The *y*-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the *x*-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the *y*-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

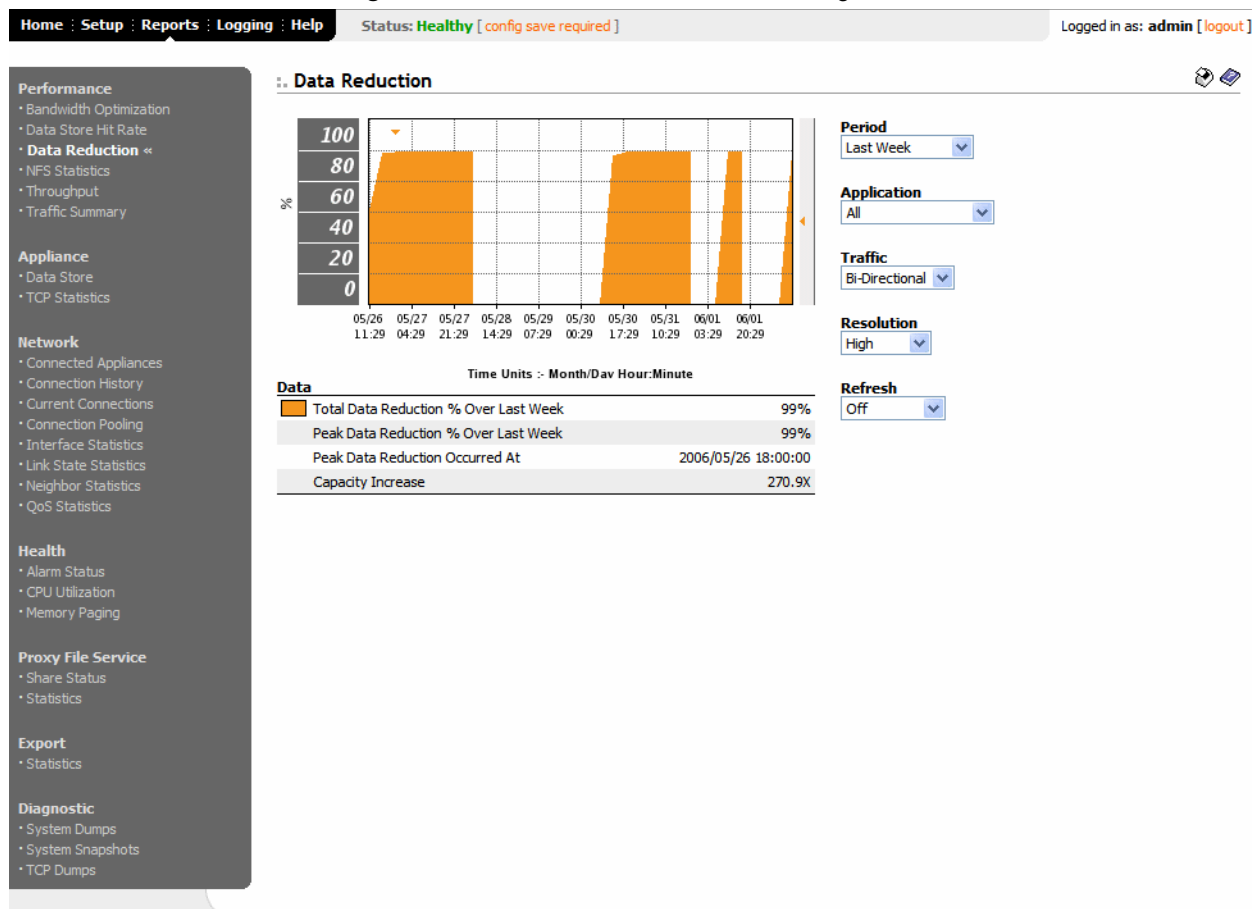
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

## To create the Data Reduction report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Performance in the left menu, click Data Reduction to display the Performance - Data Reduction page.

**Figure 3-3. Performance - Data Reduction Page**



3. Use the controls to customize the report, as described in the following table.

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Application	Select <b>FTP</b> , <b>HTTP</b> , <b>CIFS:NetBIOS</b> , <b>CIFS:TCP</b> , or <b>MAPI</b> from the drop-down list. The default value is <b>All</b> .
Traffic	Select <b>Bi-directional</b> , <b>WAN-to-LAN</b> , or <b>LAN-to-WAN</b> from the drop-down list.
Resolution	Select <b>High</b> , <b>Medium</b> , or <b>Low</b> from the <b>Resolution</b> drop-down list. <b>High</b> (small bars) allows you to drill down to specific points in time, while <b>Low</b> (large bars) enables you to count or compare aggregate values in the time interval.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>To turn off refresh, click <b>Off</b>.</li> </ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating NFS Statistics Report

The Performance - NFS Statistics report summarizes NFS optimization statistics for the time period specified.

The Performance - NFS Statistics report contains the following table of statistics that summarize data store activity.

Field	Description
Local Response	Specifies the local response time for the NFS server.
Remote Response	Specifies the total delay for NFS data.
Reduction % Over Last Month	Specifies the percentage decrease in data transmitted over the WAN.
Peak Reduction % Over Last Month	Specifies the peak-percentage decrease in data transmitted over the WAN.
Peak Reduction Occurred At	Specifies the date and time the reduction occurred.
Capacity Increase	Specifies the increase in the amount of data that can be transmitted over the WAN.

## What This Report Tells You

The Performance - NFS Statistics report answers the following questions:

- ◆ What was the local and remote response for NFS data?
- ◆ How much data was transmitted over the WAN?
- ◆ What was the overall decrease in data transmitted over the WAN?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

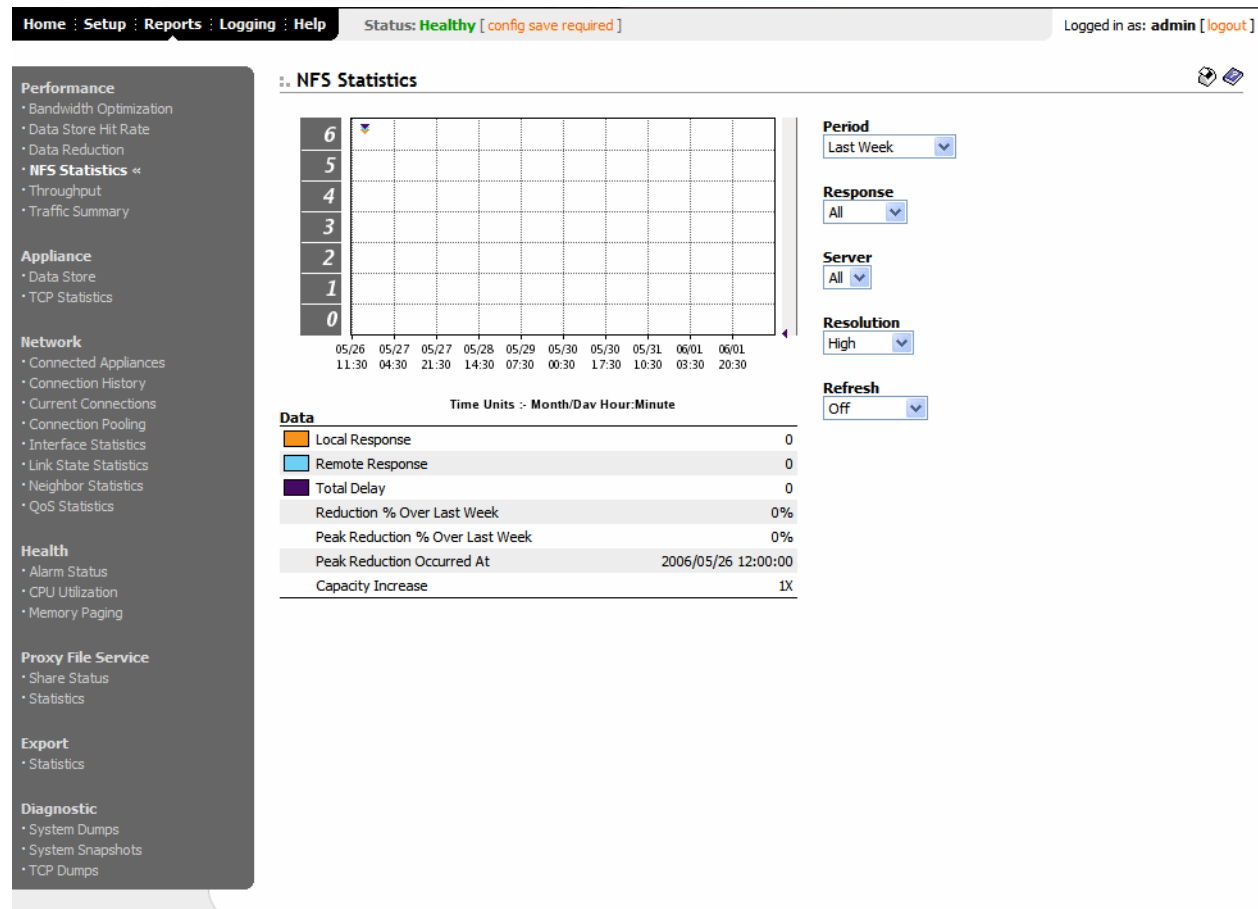
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

## To create the NFS Statistics report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Performance in the left menu, click NFS Statistics to display the Performance - NFS Statistics page.

**Figure 3-4. Performance - NFS Statistics Page**



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Response	Select <b>All</b> , <b>Local</b> , <b>Remote</b> , or <b>Delayed</b> from the drop-down list. The default value is <b>All</b> .
Server	Select the server for which you want to collect statistics from the drop-down list.
Resolution	Select <b>High</b> , <b>Medium</b> , or <b>Low</b> from the <b>Resolution</b> drop-down list. <b>High</b> (small bars) allows you to drill down to specific points in time, while <b>Low</b> (large bars) enables you to count or compare aggregate values in the time interval.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>To turn off refresh, click <b>Off</b>.</li> </ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating Throughput Reports

The Performance: Throughput report summarizes the throughput or total data transmitted for the application and time period specified.

The Performance - Throughput report includes the following table of statistics that describe data activity for the application and the time period you specify.

Field	Description
Average Throughput Over Last Week	Specifies the average amount of data transmitted.
95th Percentile Throughput Over Last Week	Specifies the 95th percentile for data activity. The 95th percentile is calculated by taking the peak of the lower 95% of inbound and outbound throughput samples.
Peak Throughput Over Last Week	Specifies the peak data transmitted in the time period specified.
Peak Throughput Occured At	Specifies when the peak data activity occurred.

## What This Report Tells You

The Performance - Throughput report answers the following questions:

- ◆ What was the average throughput?
- ◆ What was the peak throughput?
- ◆ At what time did the peak throughput occur?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the Throughput report

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Performance in the left menu, click Throughput to display the Performance - Throughput page

Figure 3-5. Performance - Throughput Page



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Application	Select <b>FTP</b> , <b>HTTP</b> , <b>CIFS:NetBIOS</b> , <b>CIFS:TCP</b> , or <b>MAPI</b> from the drop-down list. The default value is <b>All</b> .
Traffic	Select <b>Bi-directional</b> , <b>WAN-to-LAN</b> , or <b>LAN-to-WAN</b> from the drop-down list.
Resolution	Select <b>High</b> , <b>Medium</b> , or <b>Low</b> from the <b>Resolution</b> drop-down list. <b>High</b> (small bars) allows you to drill down to specific points in time, while <b>Low</b> (large bars) enables you to count or compare aggregate values in the time interval.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>• To turn off refresh, click <b>Off</b>.</li> </ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating Traffic Summary Reports

The Performance - Traffic Summary report provides a percentage breakdown of the amount of traffic going through the system by application.

The HP EFS WAN Accelerator automatically discovers all the ports in the system that have traffic. The discovered port along with a label (if one exists) is added to the report. If a label does not exist then an **unknown** label is added to the discovered port.

If you want to change the **unknown** label to a name representing the port, you must add the port with new label. All statistics for this new port label are preserved from the time the port was discovered. For detailed information about adding port labels, see [“Creating Port Labels” on page 113](#).

---

**NOTE:** The Performance - Traffic Summary report displays a maximum of 16 colors for ports. If you have more than 16 ports, the colors in the report wrap from the beginning.

---

The Performance - Traffic Summary report contains the following table of statistics that summarize traffic activity by network protocol.

Field	Description
Total Traffic	Specifies the total amount of traffic transmitted.
FTP (21)	Specifies the amount of File Transfer Protocol (FTP) data transmitted. (This also includes FTP data from other ports.)
HTTP (80)	Specifies the amount of Hypertext Transfer Protocol (HTTP) data transmitted.
CIFS: NetBIOS (139)	Specifies the amount of data transmitted with Network Basic Input Output System (NETBIOS) over the Common Internet File System (CIFS) protocol.
CIFS: TCP (445)	Specifies the amount of data transmitted with the CIFS protocol over Transmission Control Protocol (TCP).
MAPI (7830)	Specifies the amount of data transmitted over Mail Application Programming Interface (MAPI).
Other (Optimized)	Specifies the amount of data transmitted over other applications.
Passed Through (Unoptimized)	Specifies the amount of traffic transmitted unoptimized.

**NOTE:** To monitor traffic other than the default traffic listed above, see [“Setting Monitored Ports” on page 121](#).

## What This Report Tells You

The Performance - Traffic Summary report answers the following questions:

- ◆ How much data reduction occurred with a particular network protocol?
- ◆ How much data was transmitted optimized?
- ◆ How much data was transmitted unoptimized?
- ◆ How much data was transmitted using common network protocols?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.



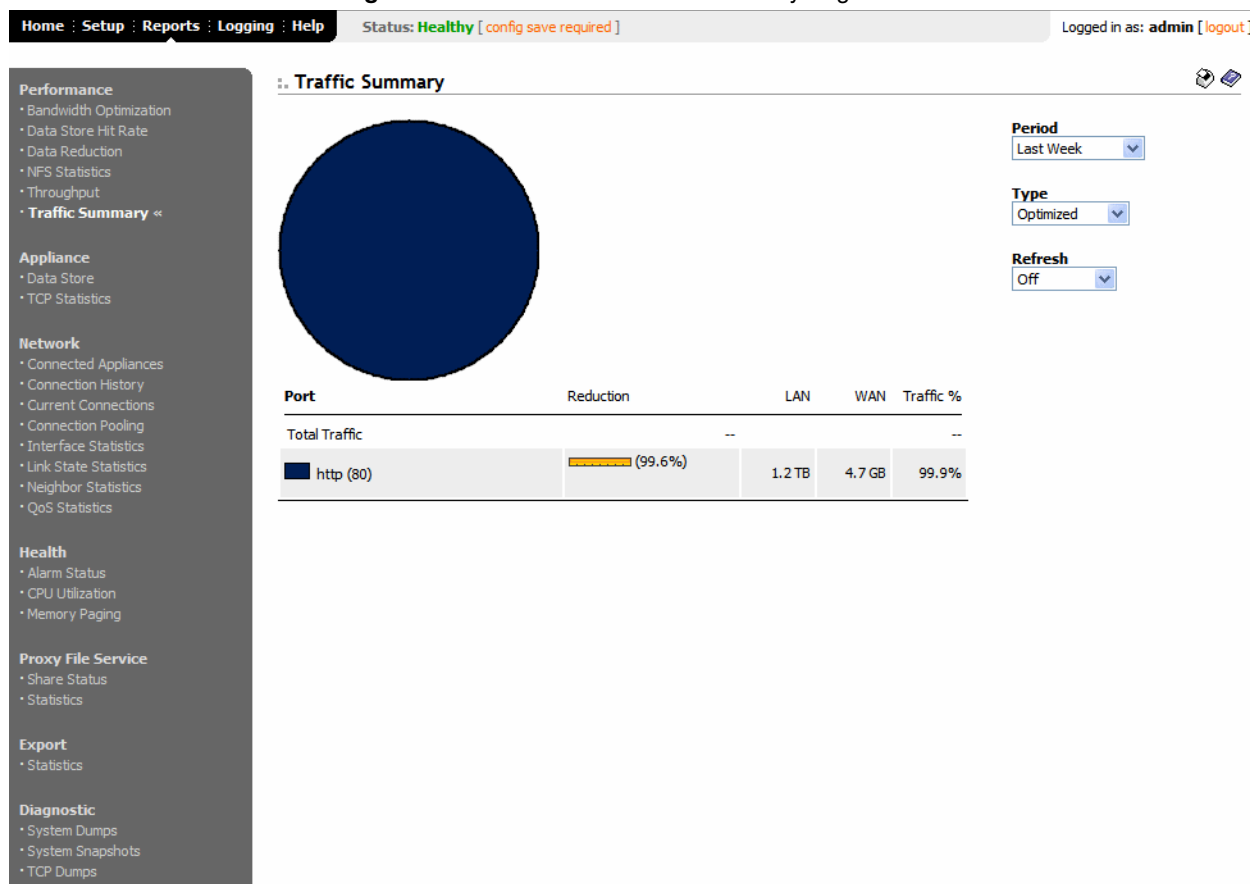
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

## To create the Traffic Summary report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Performance in the left menu, click Traffic Summary to display the Performance - Traffic Summary page.

**Figure 3-6. Performance - Traffic Summary Page**



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Type	Select <b>Optimized</b> , <b>Pass-Through</b> , or <b>Both</b> from the drop-down list. The default value is <b>Optimized</b> .
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Viewing Appliance Reports

The following section describes how to create and view appliance reports. It includes the following sections:

- ◆ [“Viewing Data Store Reports,”](#) next
- ◆ [“Viewing TCP Statistics Report”](#) on page 163

### Viewing Data Store Reports

The Appliance - Data Store report summarizes the current status and state of the data store synchronization process.

If you have enabled data store synchronization, it summarizes the state of the replication process. For detailed information, see [“Enabling Failover and Data Store Synchronization”](#) on page 73.

The Appliance - Data Store report contains the following table that summarizes the current state of the data store in the appliance.

Field	Description
Synchronization Connection Status	Specifies the current connection status of the data store.
Synchronization Catch-Up Status	Specifies the process of transferring the newest data in from the active HP EFS WAN Accelerator to the passive HP EFS WAN Accelerators. The process is complete when the <b>Catch Up</b> and <b>Keep Up</b> processes meet.
Synchronization Keep-Up Status	Specifies the process of over-writing the oldest part of the data store and proceeding to the newest part of the data store. The process is complete when the <b>Catch Up</b> and <b>Keep Up</b> processes meet.
Data Store Percentage Used (Since Last Clean)	Specifies the percentage of the data store that is available for optimization since the last data store clean request.

## What This Report Tells You

The Appliance - Data Store report answers the following questions:

- ◆ Do I have a current connection with my active HP EFS WAN Accelerator?
- ◆ How much synchronization has occurred on the data store since the synchronization request?
- ◆ What percentage of the data store is unused?

## To create the Data Store report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Appliance in the left menu, click Data Store to display the Network - Connected Appliances page.

**Figure 3-7. Appliance - Data Store Page**

The screenshot shows the HP EFS WAN Accelerator Management Console interface. The top navigation bar includes links for Home, Setup, Reports, Logging, and Help. The status is shown as 'Healthy' with a note '[ config save required ]'. The user is logged in as 'admin' with a 'logout' link. The left sidebar contains a menu with categories: Performance, Appliance, Network, Health, Proxy File Service, Export, and Diagnostic. The 'Appliance' category is expanded, showing 'Data Store' as the selected item. The main content area is titled 'Data Store' and includes a lightbulb icon with the text 'This page shows status information on the Data Store.' Below this is a table titled 'Status' with the following data:

Status	
Synchronization Connection Status	Disconnected
Synchronization Catch-Up Status	Disconnected
Synchronization Keep-Up Status	Disconnected
Data Store Percentage Used (Since Last Clean)	0.0

**TIP:** To print your report, click the **Printer** icon in the upper right corner of the page.

## Viewing TCP Statistics Report

The Appliance - TCP Statistics report summarizes TCP statistics for the appliance.

The Appliance - TCP Statistics report contains the following table of statistics that summarize TCP activity.

Packet Type	Description
Packets Received	Specifies the total packets received.
Packets Sent	Specifies the total TCP packets sent.
Packets Retransmitted	Specifies the total TCP packets retransmitted.
Timeouts	Specifies the number of time-outs.
Loss Events	Specifies the total number of loss events.

## What This Report Tells You

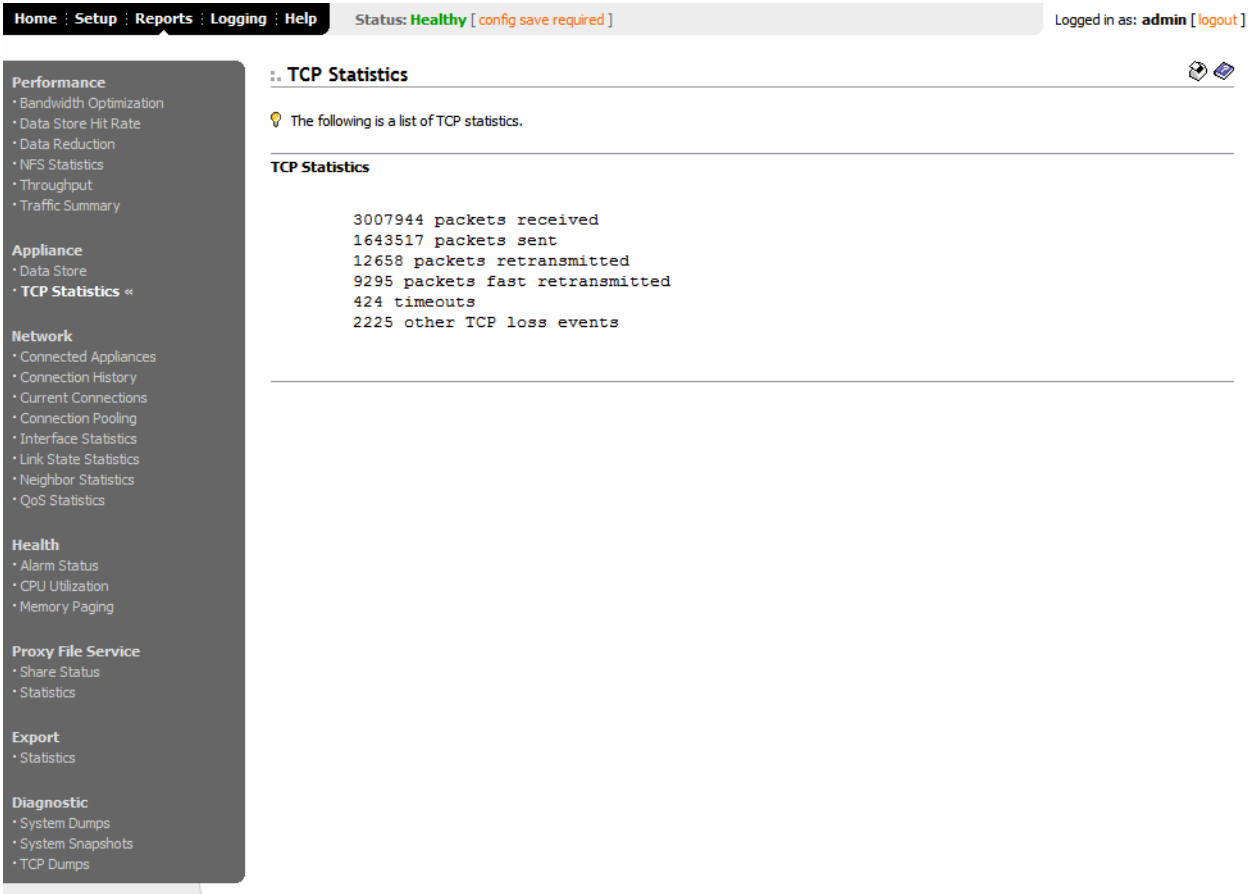
The Appliance - TCP Statistics report answers the following questions:

- ◆ How many TCP packets have been sent and received?
- ◆ How many TCP packets have been retransmitted?
- ◆ How many timeouts have occurred?
- ◆ How many loss events have occurred?

### To create the TCP Statistics report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Appliance in the left menu, click TCP Statistics to display the Network - TCP Statistics page.

Figure 3-8. Appliance - TCP Statistics Page



**TIP:** To print your report, click the **Printer** icon in the upper right corner of the page.

## Viewing Networking Reports

The following section describes how to create and view networking reports. It includes the following sections:

- ◆ “Viewing Connected Appliances Reports,” next
- ◆ “Viewing Connection History” on page 167
- ◆ “Viewing Current Connections” on page 170
- ◆ “Viewing the Current Connection Details Report” on page 172
- ◆ “Viewing Connection Pooling” on page 174

- ◆ [“Viewing Interface Statistics” on page 177](#)
- ◆ [“Creating Link State Reports” on page 178](#)
- ◆ [“Creating Neighbor Statistic Reports” on page 181](#)
- ◆ [“Creating QoS Statistics Reports” on page 182](#)

## Viewing Connected Appliances Reports

The Network - Connected Appliances report lists the connected remote HP EFS WAN Accelerators that are connected to the HP EFS WAN Accelerator.

---

**NOTE:** HP EFS WAN Accelerators might remain for a short time in the Network - Connected Appliances report after they have been shut down or renamed.

---

## What This Report Tells You

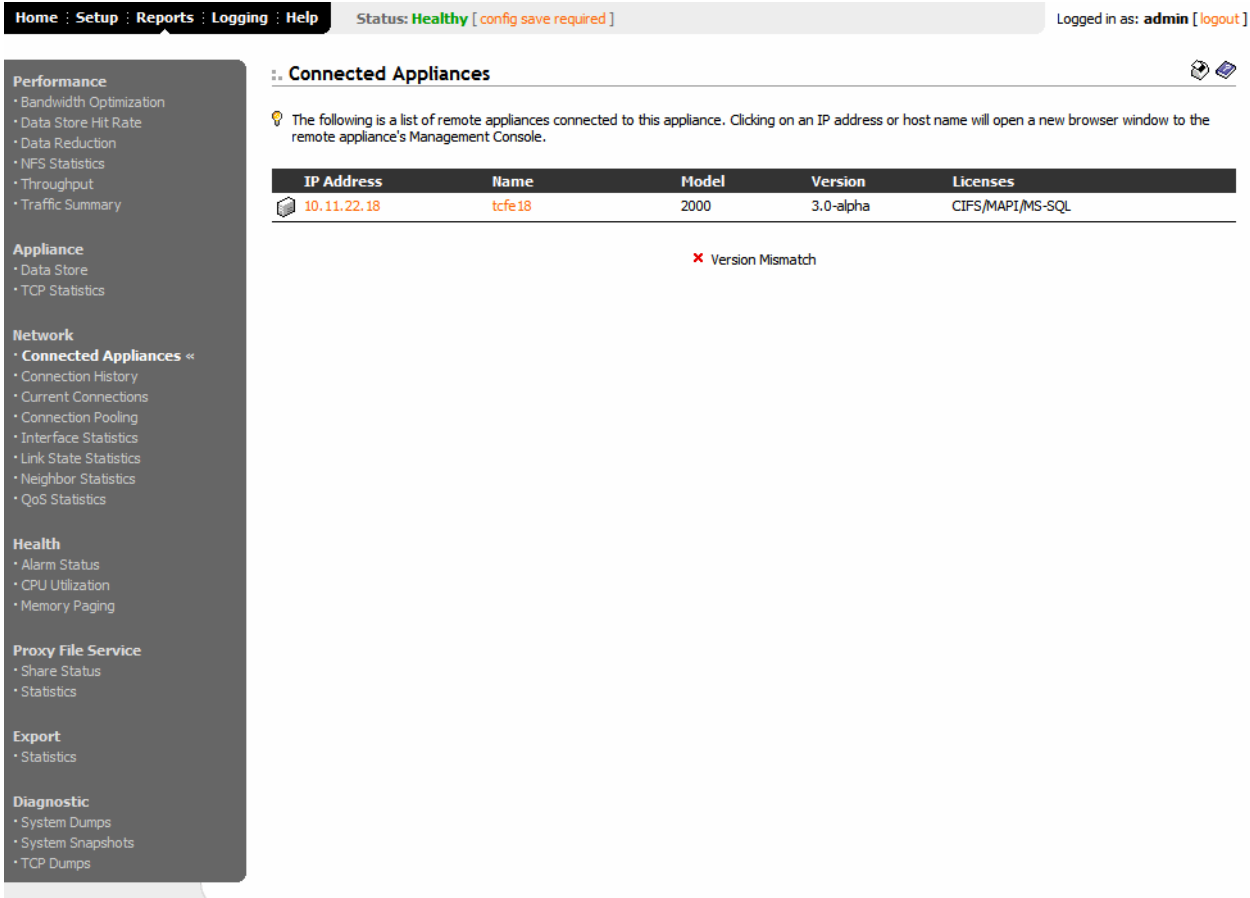
The Network - Connected Appliances report answers the following questions:

- ◆ What remote HP EFS WAN Accelerators are connected to this HP EFS WAN Accelerator?
- ◆ Is there an incompatibility issue between the HP EFS WAN Accelerator software versions.

To create the  
Connected Appliances  
report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Network in the left menu, click Connected Appliances to display the Network - Connected Appliances page.

Figure 3-9. Network - Connected Appliances Page



**TIP:** Click the appliance name or IP address in the Connected Appliance list to open the Management Console for the specified system in a new browser window.

**TIP:** To print your report, click the **Printer** icon in the upper right corner of the page.

Viewing  
Connection  
History

The Network - Connection History report summarizes the current active, established, passed-through, and active-optimized connections. The Network - Connection History report also summarizes half-opened and half-closed connections which can help you assess whether your HP EFS WAN Accelerator is appropriately sized for your network load.

The Network - Connection History report contains the following table of statistics that summarize connection activity.

Packet Type	Description
Optimized Connections	Specifies the total active connections optimized.
Flowing Connections	Specifies the total established active connections.
Half Opened	<p>Specifies the total half-opened active connections. A half-opened connection is a TCP connection in which the connection has not been fully established. Half-opened connections count toward the connection count limit on the HP EFS WAN Accelerator because, at any time, they might become a fully-opened connection.</p> <p>If you are experiencing a large number of half-opened connections, you might consider a more appropriately sized HP EFS WAN Accelerator.</p>
Half Closed	<p>Specifies the total half-closed active connections. Half-closed connections are connections which the HP EFS WAN Accelerator has intercepted and optimized but are in the process of becoming inactive. These connections are counted toward the connection count limit on the HP EFS WAN Accelerator. (Half closed connections might remain if the client or server does not close their connections cleanly.)</p> <p>If you are experiencing a large number of half-closed connections, you might consider a more appropriately sized HP EFS WAN Accelerator.</p>
Active Optimized	Specifies the total number of optimized connections with traffic in the last 60 seconds.
Pass-Through	Specifies the total connections passed through, unoptimized, when the connection limit has been reached.

## What This Report Tells You

The Network - Connection History report answers the following questions:

- ◆ How many connections were optimized?
- ◆ How many connections were passed through, unoptimized?
- ◆ How many connections were half-opened?
- ◆ How many connections were half-closed?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.



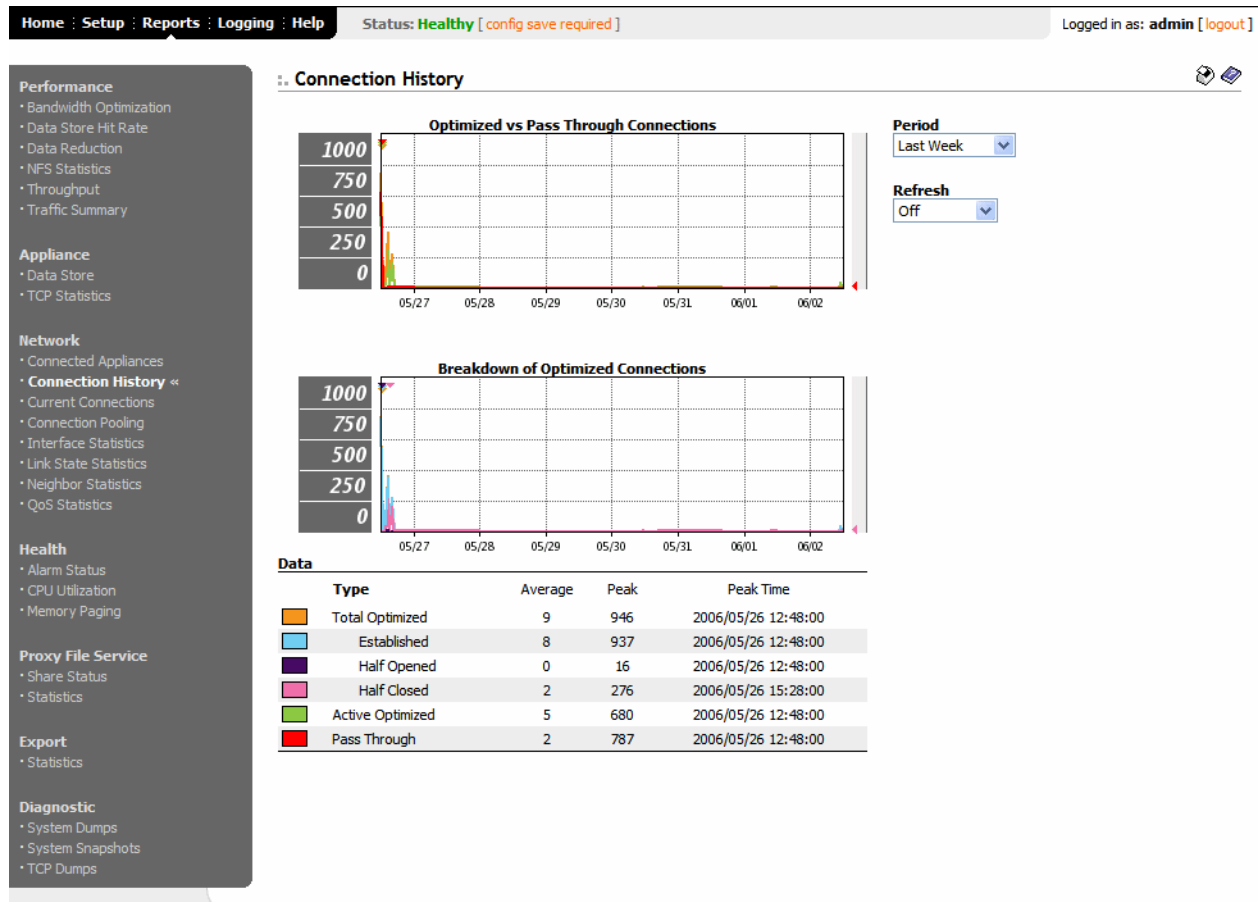
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

### To create the Connection History report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Network in the left menu, click Connection History to display the Network - Connection History page.

**Figure 3-10. Network - Connection History Page**



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>• To turn off refresh, click <b>Off</b>.</li> </ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Viewing Current Connections

The Network - Current Connections report displays the connections that are intercepted through the HP EFS WAN Accelerator, including the connections that are passed through unoptimized.

The Network - Current Connections report contains the following Current Connections table of statistics that summarize current connections.

Packet Type	Description
Established	Specifies the total established active connections.
Half Opened	<p>Specifies the total half-opened active connections. A half-opened connection is a TCP connection in which the connection has not been fully established. Half-opened connections count toward the connection count limit on the HP EFS WAN Accelerator because at any time they might become a fully opened connection.</p> <p>If you are experiencing a large number of half-opened connections, you might consider a more appropriately sized HP EFS WAN Accelerator.</p>
Half Closed	<p>Specifies the total half-closed active connections. Half-closed connections are connections which the HP EFS WAN Accelerator has intercepted and optimized but are in the process of becoming inactive. These connections are counted toward the connection count limit on the HP EFS WAN Accelerator. (Half closed connections might remain if the client or server does not close their connections cleanly.)</p> <p>If you are experiencing a large number of half-closed connections, you might consider a more appropriately sized HP EFS WAN Accelerator.</p>
Pass-Through	Specifies the total connections passed through, unoptimized when the connection limit has been reached.
Forwarded	Specifies the total number of connections that were forwarded when you have configured a connection forwarding neighbor to manage the connection.

The Network - Current Connections report also contains the following Discarded/Denied Connections table of statistics that summarize discarded or denied connections.

Packet Type	Description
Discarded	Specifies the total number of discarded connections. Discarded packets for the connection that match the Discard rule are dropped silently.
Denied	Specifies the total number of denied connections. (When packets for connections match a Deny rule, the appliance actively tries to reset the connection.)

**NOTE:** If the connection is in an unknown state, the line is greyed-out.

## What This Report Tells You

The Network - Current Connections report answers the following questions:

- ◆ How many connections were established?
- ◆ How many connections were half-opened?
- ◆ How many connections were half-closed?
- ◆ How many connections were denied or discarded?

## To create the Current Connections report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Network in the left menu, click Current Connections to display the Network - Current Connections page.

**Figure 3-11. Network - Current Connections Page**

Home : Setup : **Reports** : Logging : Help      Status: **Healthy** [ config save required ]      Logged in as: **admin** [ logout ]

**Performance**

- Bandwidth Optimization
- Data Store Hit Rate
- Data Reduction
- NFS Statistics
- Throughput
- Traffic Summary

**Appliance**

- Data Store
- TCP Statistics

**Network**

- Connected Appliances
- Connection History
- **Current Connections** «
- Connection Pooling
- Interface Statistics
- Link State Statistics
- Neighbor Statistics
- QoS Statistics

**Health**

- Alarm Status
- CPU Utilization
- Memory Paging

**Proxy File Service**

- Share Status
- Statistics

**Export**

- Statistics

**Diagnostic**

- System Dumps
- System Snapshots
- TCP Dumps

**Connections**

The following is a list of connections currently handled by this appliance.

Filter:  Type: All

T	Source:Port	Dest:Port	Reduction	KBytes LAN/WAN	Since	App	Notes
Q >>>	10.11.1.1:33680	10.11.100.100:80	<div><div></div></div> (99%)	6307 KB/45 KB	2006/06/02 11:55:23	TCP	
Q >>>	10.11.1.1:33681	10.11.100.101:80	<div><div></div></div> (99%)	4242 KB/6 KB	2006/06/02 11:55:24	TCP	
Q >>>	10.11.1.1:33682	10.11.100.102:80	<div><div></div></div> (99%)	1439 KB/1 KB	2006/06/02 11:55:25	TCP	

/ SDR Enabled    / Compression Enabled    / Protocol Error

**Connection Counts**

>>> Established (Optimized)	3
>>>> Half Opened (Optimized)	0
>>>> Half Closed (Optimized)	0
>>> Pass Through	0
>>> Forwarded	0
<b>Total</b>	<b>3</b>

**Discarded/Denied Connections**

Discarded	0
Denied	0
<b>Total</b>	<b>0</b>

---

**NOTE:** If the connection is in an unknown state, the line is greyed-out.

---

3. Use the controls to customize the report, as described in the following table..

Control	Description
Filter	Specify an IP address or port number in the <b>Filter</b> text box to filter the report.
Type	<p><b>All.</b> Specifies all established active connections.</p> <ul style="list-style-type: none"><li>• <b>Established (Optimized) Only.</b> Specifies the total established active connections.</li><li>• <b>Half-Opened (Optimized) Only.</b> Specifies the total half-opened active connections. A half-opened connection is a TCP connection in which the connection has not been fully established. Half-opened connections count toward the connection count limit on the appliance because at any time they might become a fully opened connection. If you are experiencing a large number of half-opened connections, you might consider a more appropriately sized system.</li><li>• <b>Half-Closed (Optimized) Only.</b> Specifies the total half-closed active connections. Half-closed connections are connections which the appliance has intercepted and optimized but are in the process of becoming inactive. These connections are counted toward the connection count limit on the appliance. (Half closed connections might remain if the client or server does not close their connections cleanly.) If you are experiencing a large number of half-closed connections, you might consider a more appropriately sized system.</li><li>• <b>Pass-Through Only.</b> Specifies the total connections passed through, unoptimized when the connection limit has been reached.</li><li>• <b>Forwarded.</b> Specifies the total number of connections that were forwarded when you have configured a connection forwarding neighbor to manage the connection.</li></ul>
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

---

**NOTE:** If you have the Secure-CIFS feature enabled (which disables Server Message Block (SMB) signing), the Network - Current Connections report displays Protocol Error—this is an expected response. For detailed information about enabling Secure-CIFS, see [“Configuring CIFS Protocol Support” on page 31](#).

---

## Viewing the Current Connection Details Report

The Network - Current Connections: Connection Details report displays details about the connected HP EFS WAN Accelerator such as the source and destination IP address, the peer HP EFS WAN Accelerator, the inner local port, and so forth.

The Network - Current Connections report contains the following table that summarizes current connection details.

Field	Description
Type	Specifies the type of connection.
Source	Specifies the source IP address for the connection.
Destination	Specifies the destination IP address for the connection.
Peer Appliance	Specifies the IP address of the remote HP EFS WAN Accelerator the connection is going through.
Inner Local Port	Specifies the local port for the inner connection to the peer HP EFS WAN Accelerator.
Outer Local	Specifies the local port for the outer connection to the client or server.
Outer Remote	Specifies the remote port for the outer connection to the client or server.
Client-Side	Specifies whether the connection is a client-side HP EFS WAN Accelerator for this connection.
Since	Specifies the time the system has been active.
App	Specifies the internal protocol blade that is used to service the connection.
Bytes In (LAN)	Specifies the total number of LAN bytes for this connection.
Bytes Out (WAN)	Specifies the total number of WAN bytes for this connection.
Reduction	Specifies the percent reduction of traffic over the WAN.

## What This Report Tells You

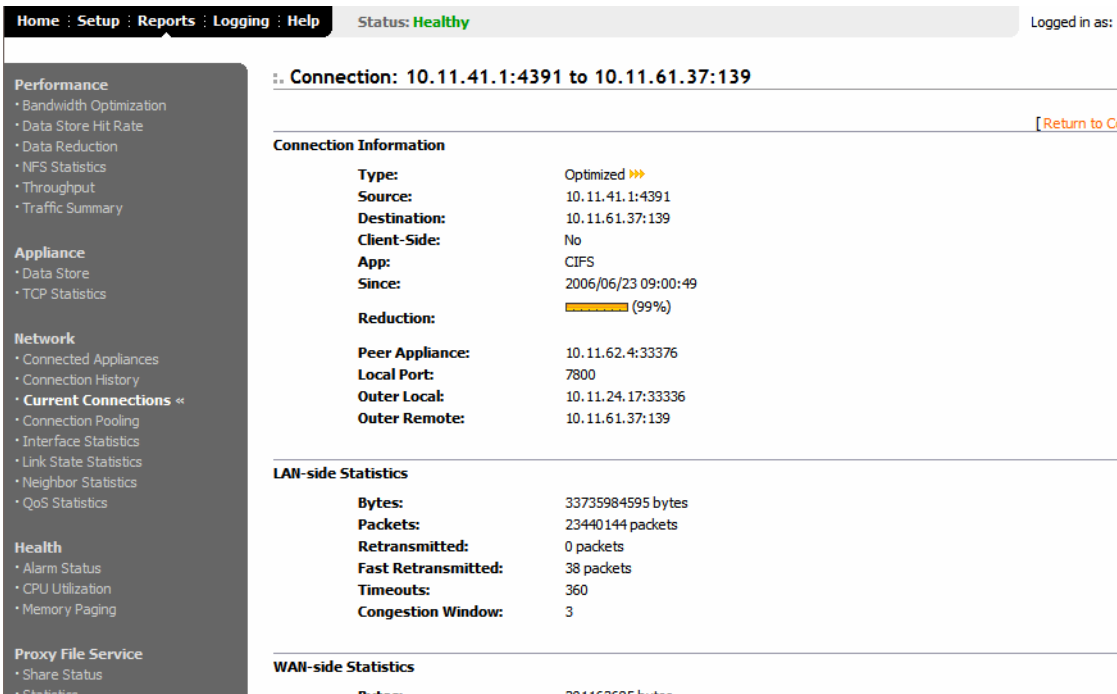
The Network - Current Connections Detail report answers the following questions:

- ◆ How is the status of this system?
- ◆ What is the peer for this system?
- ◆ What are the total number of bytes in and out of this system?
- ◆ What is the percent reduction of traffic for this system?

To view current connection details

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Network in the left menu, click Current Connections to display the Network - Current Connections page.
- 3. Click the magnifying-glass next to the HP EFS WAN Accelerator name to display the Network - Current Connections Details page.

Figure 3-12. Network - Current Connections Details Page



**TIP:** To send keep-alive messages for this system, click **Send Keep Alive**. To reset keep-alive messages for the system, click **Reset**.

Viewing Connection Pooling

The Network - Connection Pooling report summarizes the current connection pool of connections to peer appliances.

The Network - Current Connections report contains the following table that summarizes current connection details.

Field	Description
Total Pool	Specifies the total pool of connections to peer appliances.
Total Hits	Specifies the total number of successful connections.
Peak Hits	Specifies the peak number of successful connections in the time period specified.
Peak Hits Occurred At	Specifies the date and time of the peak number of connections.

## What This Report Tells You

The Network - Connection Pooling report answers the following questions:

- ◆ How large is the pool of connections?
- ◆ How many connections occurred?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

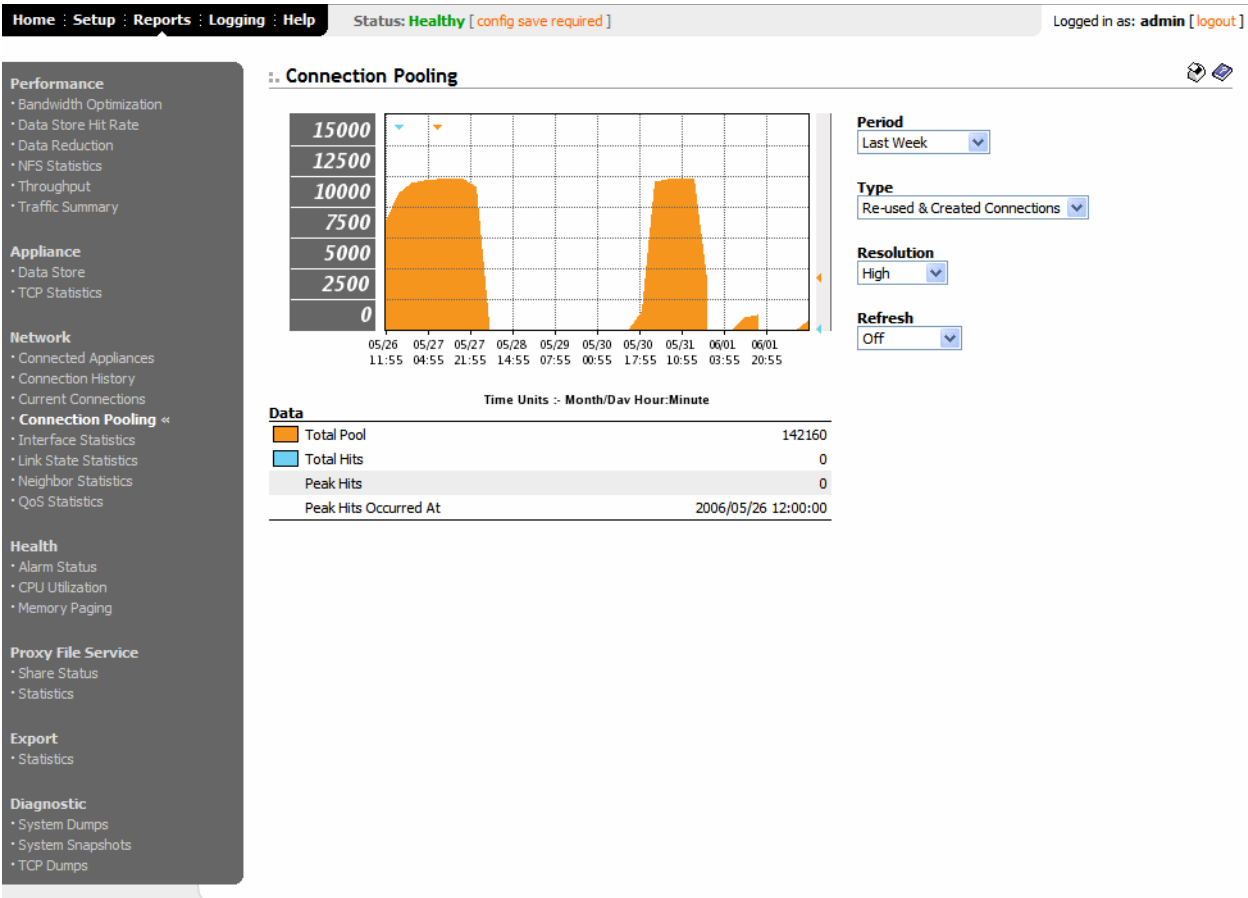
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the Connection Pooling report

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Network in the left menu, click Connection Pooling to display the Network - Connection Pooling page.

Figure 3-13. Network - Connection Pooling Page



- 3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Type	Select <b>Re-used &amp; Created Connections</b> or <b>Re-used Percentage</b> from the drop down list.
Resolution	Select <b>High</b> , <b>Medium</b> , <b>Low</b> , or <b>Maximum</b> from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.



## Viewing Interface Statistics

The Network - Interfaces Statistics report summarizes the statistics for the primary, in-path LAN and WAN, and auxiliary interfaces. It also displays the IP address, speed, duplex, MAC address, and current status for each interface.

**TIP:** For auto-negotiated speed and duplex settings the Network - Interfaces Statistics report displays the speed at which they were negotiated.

The Network - Interfaces Statistics report displays the following statistics.

	Packet Type	Description
<b>Primary Interface</b>	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, and <b>mcast</b> packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
<b>In-Path: LAN Interface</b>	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, frames sent, and <b>mcast</b> packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
<b>In-Path: WAN Interface</b>	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, frames sent, and <b>mcast</b> packets sent.
	TX Packets (Transmitted)	Specifies the number packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.
<b>Auxiliary Interface</b>	RX Packets (Received)	Specifies the number of packets discarded, errors encountered, packets overrun, and <b>mcast</b> packets sent.
	TX Packets (Transmitted)	Specifies the number of packets discarded, errors encountered, packets overrun, carriers used, and collisions encountered.

**NOTE:** If you have multiple dual port or four-port bypass cards installed, the Network - Interface Statistics report displays the interface statistics for each LAN and WAN port.

## What This Report Tells You

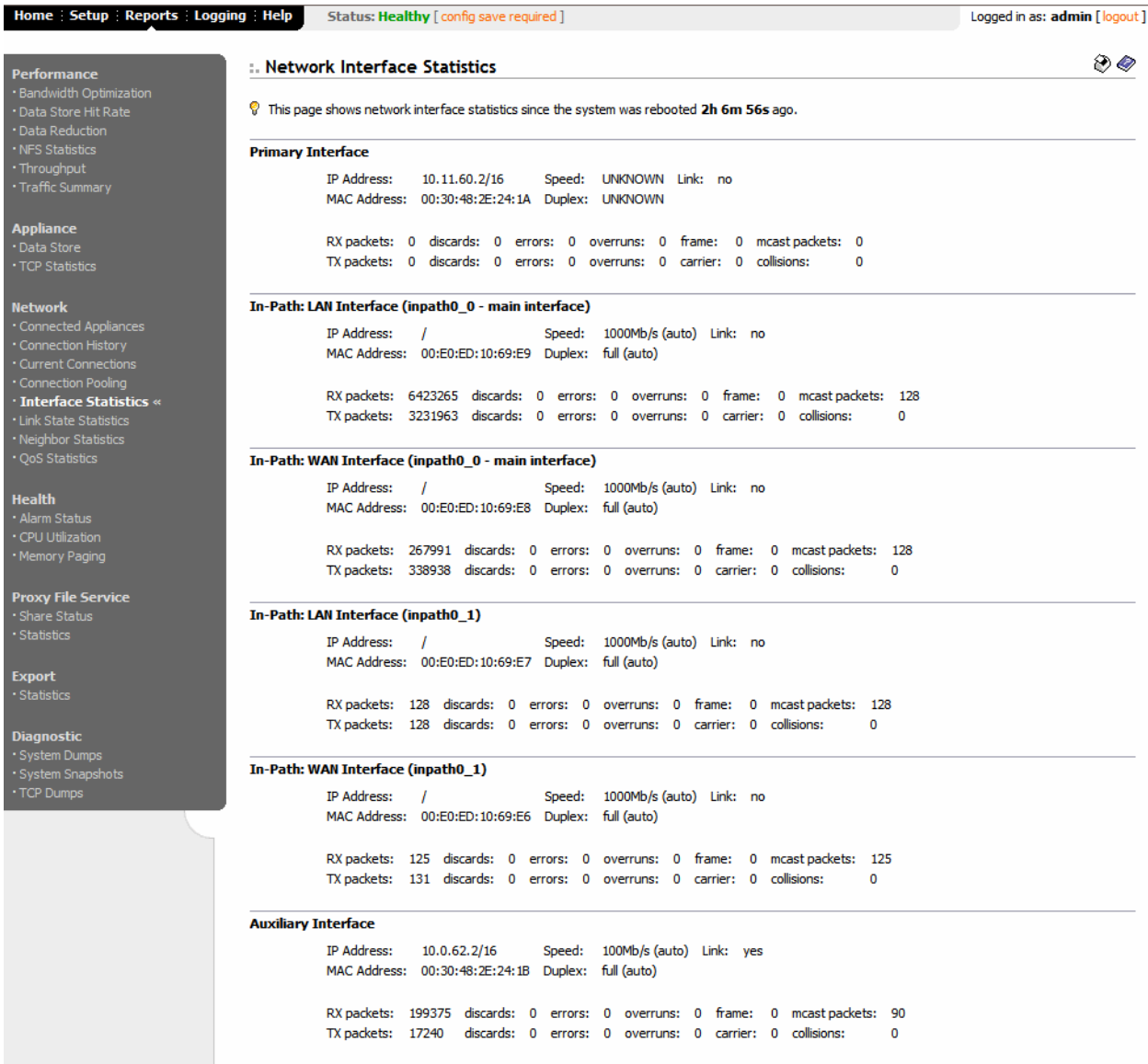
The Network - Interface Statistics report answers the following questions:

- ◆ How many packets am I transmitting?
- ◆ How many errors are there in each transmission?
- ◆ What is the current status of my interface?

To view Interface Statistics

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Network in the left menu, click Interface Statistics to display the Network - Interface Statistics page.

Figure 3-14. Network - Interface Statistics Page



**TIP:** To print your report, click the **Printer** icon in the upper right corner of the page.

Creating Link State Reports

The Network - Link State report summarizes the loss rate for the HP EFS WAN Accelerator. The loss rate is the rate at which packets are not successfully delivered to the peer HP EFS WAN Accelerator.

## What This Report Tells You

The Network - Link State report answers the following question:

- ◆ What percentage of packets did not reach the peer HP EFS WAN Accelerator?

## About Report Graphs

In bar-graph and line-graph reports, the *x*-axis (or tick mark) plots time, according to the interval you select. The *y*-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the *x*-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the *y*-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

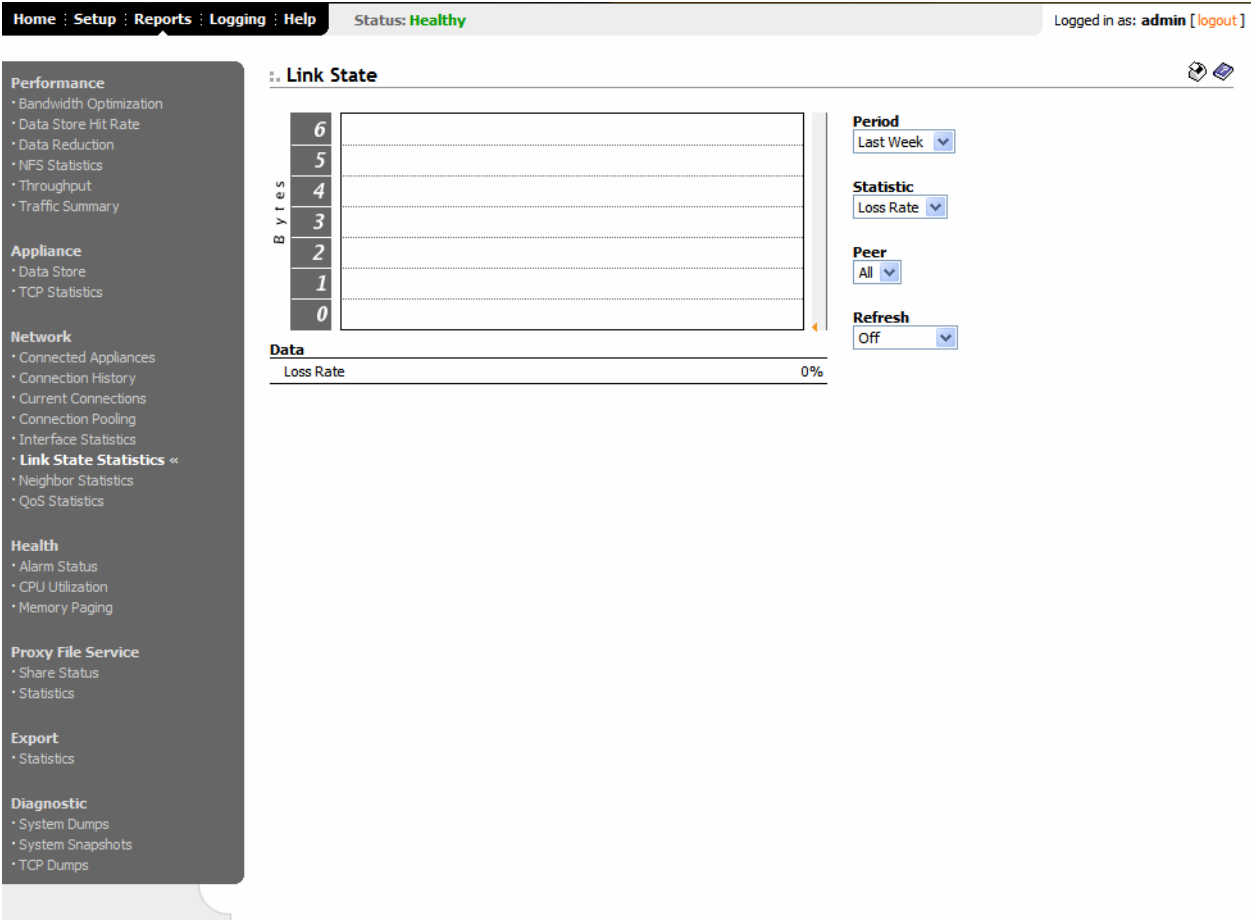
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the Link State report

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Network in the left menu, click Link State to display the Network - Link State page.

Figure 3-15. Network - Link State Page



- 3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Statistic	Select <b>Loss Rate</b> from the drop-down list.
Peer	Select <b>All</b> or a specific peer from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating Neighbor Statistic Reports

### What This Report Tells You

The Network - Neighbor Statistics report summarizes number of bytes or packets transferred between the HP EFS WAN Accelerator and a specified neighbor.

The Network - Neighbor Statistics report answers the following questions:

- ◆ How many bytes were transferred between an HP EFS WAN Accelerator and a specified neighbor?
- ◆ How many packets were transferred between an HP EFS WAN Accelerator and a specified neighbor?

### About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

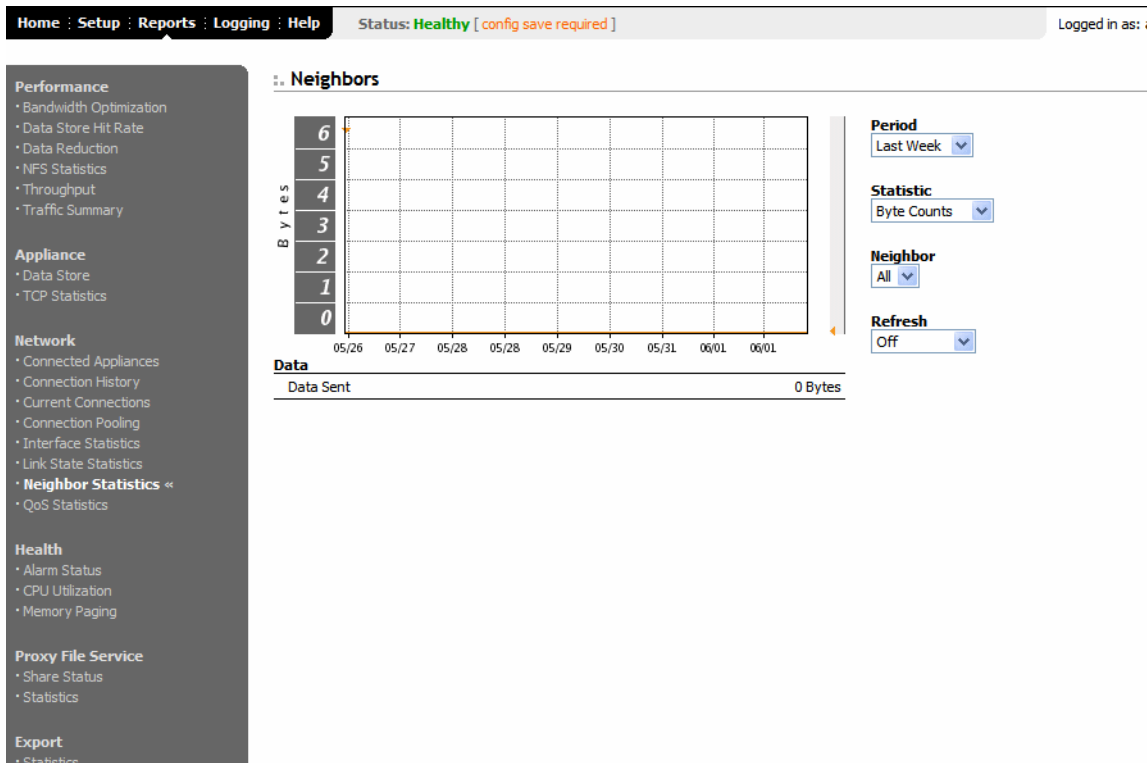
### About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the Neighbor Statistics report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Network in the left menu, click Neighbor Statistics to display the Network - Neighbor Statistics page.

Figure 3-16. Network - Neighbor Statistics Page



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Statistic	Select <b>Byte Counts</b> or <b>Packet Counts</b> from the drop-down list.
Neighbor	Select <b>All</b> or a specific neighbor from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

Creating QoS Statistics Reports

The Network - QoS Statistics report summarizes the number of bytes and packets transmitted for the QoS class or an aggregate of all classes for the time period specified.

The Network - QoS Statistics report contains the following Data table of statistics that summarize current connections.

Field	Description
Data Sent	Specifies the total amount of data sent over the WAN for the QoS class.
Data Dropped	Specifies the total amount of data packets that were dropped for the QoS class.
Peak Data % Over Last Week	Specifies the peak amount of data transmitted over the last week.
Pass Data % Occurred At	Specifies when the peak data transmission occurred.

## What This Report Tells You

The Network - QoS Statistics report answers the following questions:

- ◆ How many bytes transmitted over the WAN for the QoS class?
- ◆ How many data packets were dropped for the QoS class?
- ◆ When did the peak data transmission occur for the QoS class?

## About Report Graphs

In bar-graph and line-graph reports, the *x*-axis (or tick mark) plots time, according to the interval you select. The *y*-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the *x*-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the *y*-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

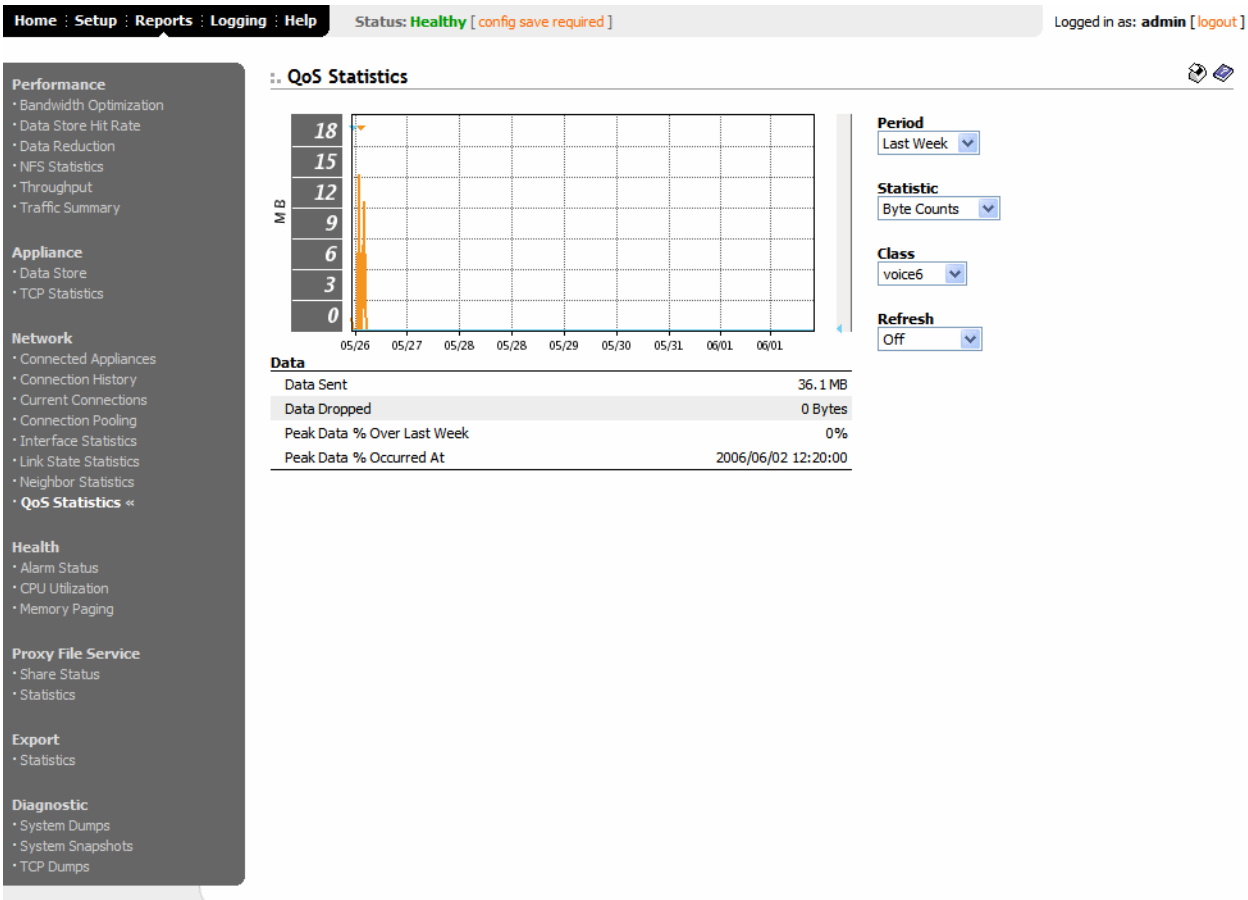
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

To create the QoS Statistics report

- 1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
- 2. Under Network in the left menu, click QoS Statistics to display the Network - QoS Statistics page.

Figure 3-17. Network - QoS Statistics Page



- 3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Statistic	Select <b>Byte Counts</b> or <b>Packet Counts</b> from the drop-down list.
Class	Select the QoS class from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.



## Viewing System Health Reports

The following section describes how to view reports that summarize the current status of the HP EFS WAN Accelerator. It includes the following sections:

- ◆ [“Viewing Alarm Status Reports,”](#) next
- ◆ [“Creating CPU Utilization Reports”](#) on page 188
- ◆ [“Creating Memory Paging Reports”](#) on page 190

### Viewing Alarm Status Reports

The Health - Alarm Status report provides status for the HP EFS WAN Accelerator alarms.

The Health -Alarm Status report contains the following table of statistics that summarize traffic activity by application.

Alarm	Description
Admission Control	Whether the system connection limit has been reached. Additional connections are passed through unoptimized. The alarm clears when the HP EFS WAN Accelerator moves out of this condition.
Asymmetric Routing	Indicates <b>OK</b> if the system is not experiencing asymmetric traffic. If the system does experience asymmetric traffic, this condition is detected and reported here. In addition, the traffic is passed through, and the route appears in the Asymmetric Routing table. For information about the Asymmetric Routing table, see <a href="#">“Enabling Asymmetric Routing Auto-Detection”</a> on page 66.
Central Processing Unit (CPU) Utilization	<p>Whether the system has reached the CPU threshold for any of the CPUs in the HP EFS WAN Accelerator. If the system has reached the CPU threshold, check your settings. For detailed information, see <a href="#">“Setting Alarm Parameters”</a> on page 116.</p> <p>If your alarm thresholds are correct, reboot the HP EFS WAN Accelerator. For detailed information, see <a href="#">“Rebooting the HP EFS WAN Accelerator”</a> on page 145.</p> <p><b>NOTE:</b> If more than 100 MB of data is moved through an HP EFS WAN Accelerator, Model 1010 while performing PFS synchronization, the CPU utilization might become high and result in a CPU alarm. This CPU alarm should not be cause for concern.</p>
Data Store	Whether the data store is corrupt. To clear the data store of data, restart the HP EFS WAN Accelerator service and click <b>Clear Data Store on Next Restart</b> . For detailed information, see <a href="#">“Starting and Stopping Services”</a> on page 144.
Licensing	Whether your licenses are current. For detailed information about updating licenses, see <a href="#">“Updating Your Licenses”</a> on page 137.
Link State	Whether the system has detected a link that is down. You are notified via SNMP traps, email, and alarm status.

Alarm	Description
Memory Paging	Whether the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours the HP EFS WAN Accelerator is functioning properly. If thousands of pages are swapped every few minutes, then reboot the HP EFS WAN Accelerator. For detailed information, see <a href="#">“Rebooting the HP EFS WAN Accelerator” on page 145</a> . If rebooting does not solve the problem, contact HP technical support.
Network Bypass	<p>Whether the system is in bypass mode. If the HP EFS WAN Accelerator is in bypass mode, restart the HP EFS WAN Accelerator service.</p> <p>If restarting the service does not resolve the problem, reboot the HP EFS WAN Accelerator. For detailed information, see <a href="#">“Rebooting the HP EFS WAN Accelerator” on page 145</a>.</p> <p>If rebooting does not resolve the problem, shutdown and restart the HP EFS WAN Accelerator. For detailed information, see <a href="#">“Rebooting the HP EFS WAN Accelerator” on page 145</a> and <a href="#">“Starting and Stopping Services” on page 144</a>.</p>
NFS V2/V4 Alarm	Whether the system has triggered a v2 or v4 NFS alarm.
Optimization Service	Whether the system has detected a software error in the HP EFS WAN Accelerator service. The HP EFS WAN Accelerator service continues to function, but an error message appears in the logs that you should investigate. For detailed information, see <a href="#">“Viewing HP EFS WAN Accelerator Logs” on page 201</a> .
Proxy File Service Partition Full	Whether you Proxy File Service (PFS) partition is full.

Alarm	Description
Proxy File Service Connection Error	Whether there has been a PFS connection error. If a connection error is detected, restart the HP EFS WAN Accelerator service and PFS. For detailed information, see <a href="#">“Enabling Proxy File Service” on page 99</a> and <a href="#">“Starting and Stopping Services” on page 144</a> .
Proxy File Service Operation Failed	Whether a synchronization operation has failed. If an operation failure is detected, attempt the operation again. For detailed information, see <a href="#">“Adding PFS Shares” on page 102</a> .
Redundant Array of Independent Disks (RAID)	<p>Whether the system has encountered RAID errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete.</p> <p><b>IMPORTANT:</b> Rebuilding a disk drive can take 4-6 hours.</p> <p><b>NOTE:</b> RAID status applies only to the HP EFS WAN Accelerator, Series 3000 and 5000.</p>
Software Version Mismatch	<p>Whether there is a mismatch between software versions in your network. If a software mismatch is detected, resolve the mismatch by upgrading or reverting to a previous version of the software. For detailed information, see <a href="#">“Upgrading Your Software” on page 142</a>.</p> <p><b>NOTE:</b> If a software version mismatch occurs and you are running v.1.2 and client-side v.2.1 HP EFS WAN Accelerators, you must set the correct version of the HP EFS WAN Accelerator service protocol on the client-side v.2.1 appliances using the HP EFS WAN Accelerator CLI:</p> <pre>sh&gt; peer &lt;addr&gt; version min 5 sh&gt; peer &lt;addr&gt; version max 5</pre>
System Disk Full	Whether the data store has reached maximum disk capacity.
Temperature	Whether the CPU temperature has exceeded the critical threshold. The default value for the rising threshold temperature is 70° C; the default reset threshold temperature is 67° C.

## What This Report Tells You

The Health -Alarm Status report answers the following question:

- ◆ What is the current status of the HP EFS WAN Accelerator?

## To create the Alarm Status report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Health in the left menu, click Alarm Status to display the Health - Alarm Status page.

**Figure 3-18. Health - Alarm Status Page**

The screenshot shows the HP EFS WAN Accelerator interface. At the top, there is a navigation bar with links: Home, Setup, Reports, Logging, and Help. The status is displayed as 'Healthy [config save required]' and the user is logged in as 'admin [logout]'. On the left, there is a sidebar menu with categories: Performance, Appliance, Network, Health, Proxy File Service, Export, and Diagnostic. Under the Health category, 'Alarm Status' is selected. The main content area is titled 'Alarm Status' and contains a message: 'The following is the status of all alarm indicators for this appliance.' Below this is a table with two columns: 'Alarm' and 'Status'.

Alarm	Status
Admission Control	[OK]
CPU Utilization	[OK]
Data Store	[OK]
Licensing	[OK]
Link State	[OK]
Memory Paging	[OK]
Network Bypass	[OK]
NFS V2/V4 Alarm	[OK]
Optimization Service	[OK]
Proxy File Service partition full	[OK]
Proxy File Service configuration error	[OK]
Proxy File Service operation failed	[OK]
RAID	[OK]
Software Version Mismatch	[OK]
System Disk Full	[OK]
Temperature	[OK]

**NOTE:** To print your report, click the **Printer** icon in the upper right corner of the page.

## Creating CPU Utilization Reports

The Health - CPU Utilization report summarizes the percentage of the CPU utilized in the time period specified.

### What this Report Tells You

The Health - CPU Utilization report answers the following questions:

- ◆ How much CPU is being used?
- ◆ What is the average and peak percentage of CPU being used?

### About Report Graphs

In bar-graph and line-graph reports, the *x*-axis (or tick mark) plots time, according to the interval you select. The *y*-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

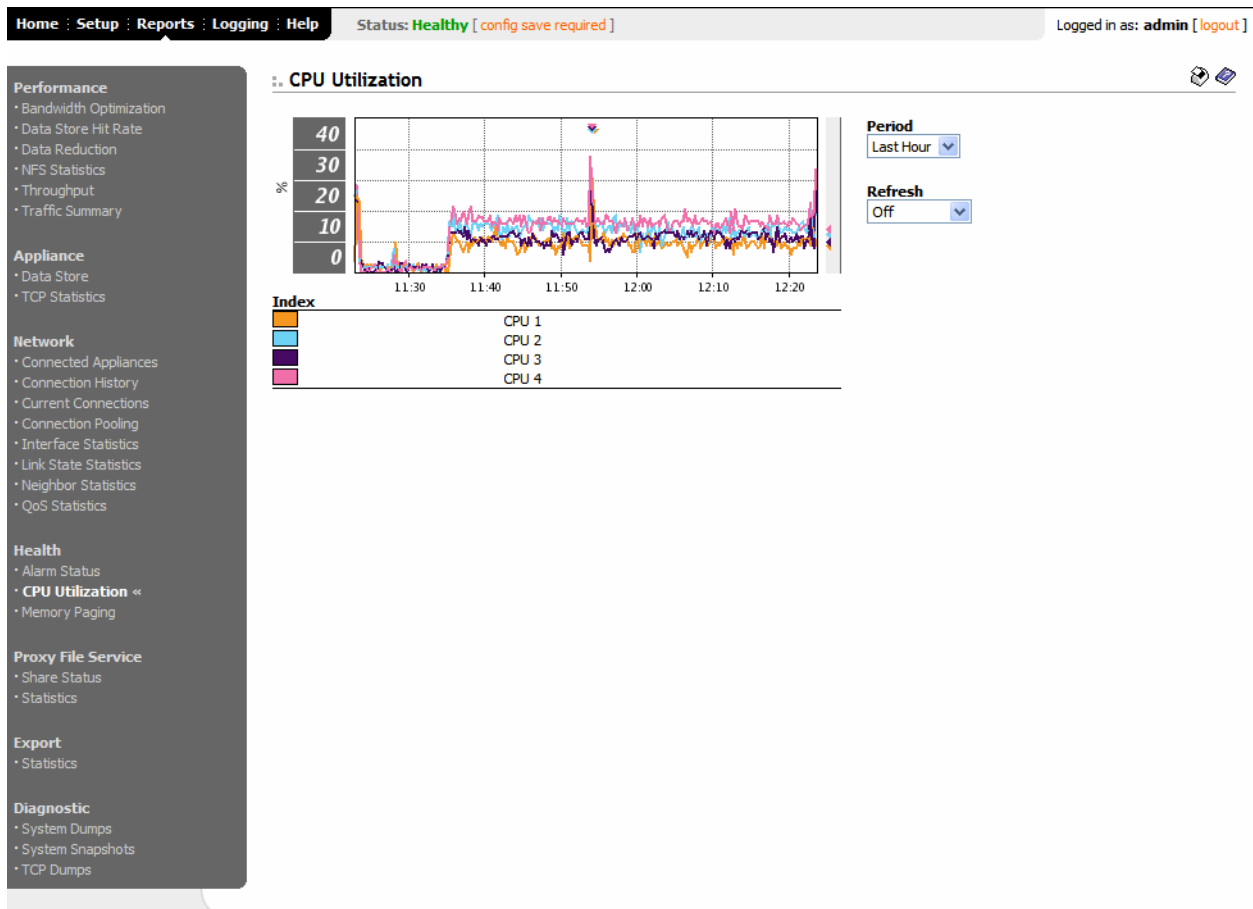
A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

## To create the CPU Utilization report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Health in the left menu, click CPU Utilization to display the Health - CPU Utilization page.

**Figure 3-19. Health - CPU Utilization Page.**



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"><li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li><li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li><li>• To turn off refresh, click <b>Off</b>.</li></ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Creating Memory Paging Reports

The Health - Memory Paging report provides the total number of memory pages, per second, utilized in the time period specified.

The Health - Memory Paging report includes the following table of statistics that describe memory paging activity for the time period you specify.

Field	Description
Total Pages Swapped Out	Specifies the total number of pages swapped. If 100 pages are swapped approximately every two hours the HP EFS WAN Accelerator is functioning properly. If thousands of pages are swapped every few minutes, contact HP technical support.
Average Pages Swapped Out	Specifies the average number of pages swapped. If 100 pages are swapped every couple of hours the HP EFS WAN Accelerator is functioning properly. If thousands of pages are swapped every few minutes, contact HP technical support.
Peak Pages Swapped Out	Specifies the peak number of pages swapped.
Peak Pages Swapped Out Occured At	Specifies the time and date that the peak number of pages were swapped.

## What this Report Tells You

The Health - Memory Paging report answers the following questions:

- ◆ How much memory is being used?
- ◆ What is the average and peak amount of memory pages swapped?

## About Report Graphs

In bar-graph and line-graph reports, the x-axis (or tick mark) plots time, according to the interval you select. The y-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the x-axis (the time) at which the peak occurred.

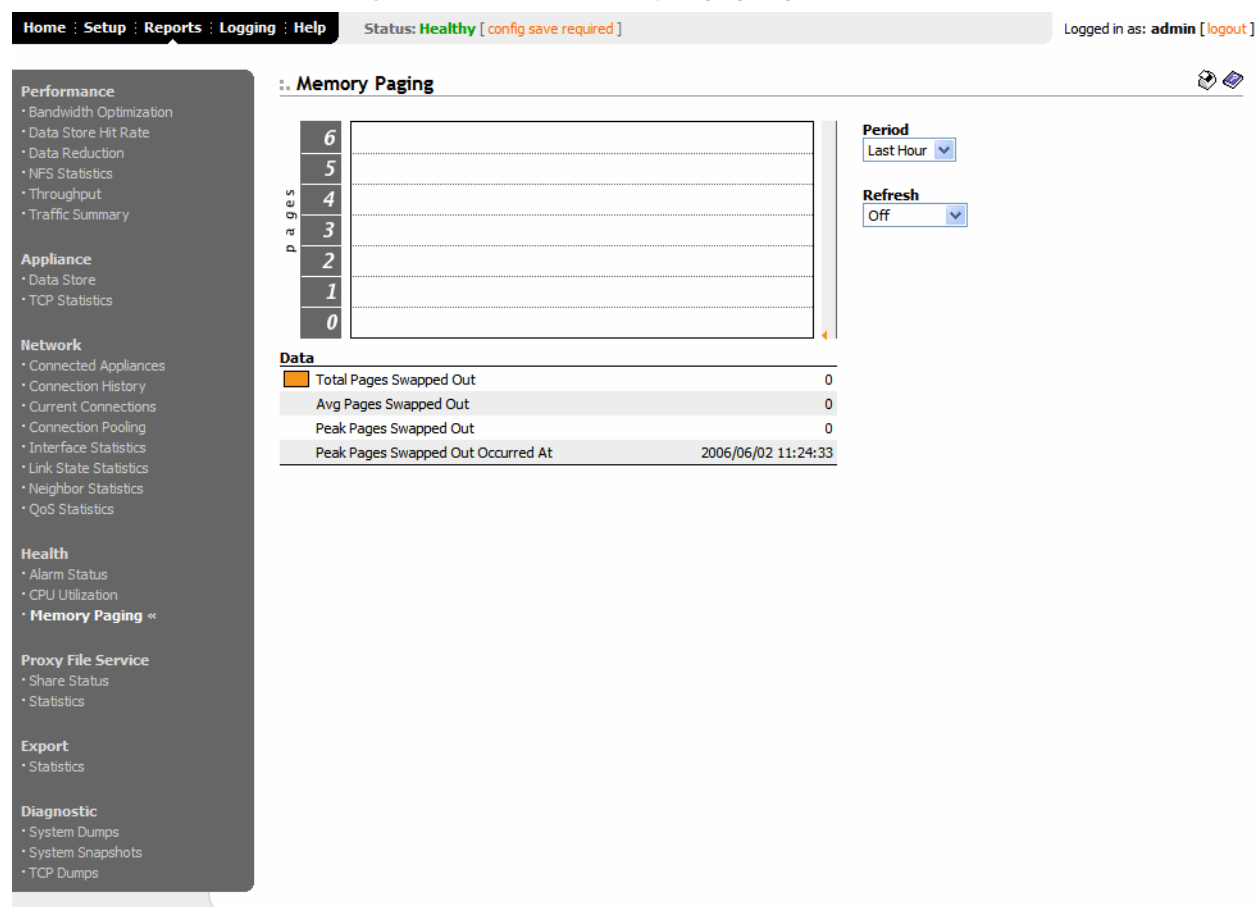
A diamond icon outside the right margin of the graph points to the value on the y-axis (for example, the percent) that is the average value for the time period selected.

## To create Memory Paging report

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Health in the left menu, click Memory Paging to display the Health - Memory Paging page.

**Figure 3-20. Health - Memory Paging Page**



3. Use the controls to customize the report, as described in the following table.

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>• To turn off refresh, click <b>Off</b>.</li> </ul> <p><b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.</p>
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

---

## Viewing Proxy File Service Reports

The following section describes the Proxy File Share (PFS) Status report. It includes the following sections:

- ◆ [“Viewing PFS Share Status Reports,”](#) next
- ◆ [“Viewing PFS Statistics”](#) on page 193

### Viewing PFS Share Status Reports

The PFS Share Status report provides information about your PFS shares: the size of the share and the status of the share. For detailed information, see [“Enabling Proxy File Service”](#) on page 99.

#### What this Report Tells You

The PFS Share Status report answers the following questions:

- ◆ What action is occurring on the share?
- ◆ How large is the share?
- ◆ Is the share ready for synchronization?
- ◆ Is a synchronization currently occurring?



## To view the PFS Share Status report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Click Share Status in the left menu to display the PFS - Share Status page.

**Figure 3-21. PFS - Share Status Page**

Home : Setup : Reports : Logging : Help    Status: **Healthy** [ config save required ]    Logged in as: admin [ logout ]

**Proxy File Service (PFS) - Shares** [ Jump to Share Configuration ]

Local Name	Enabled	Status	Size (MB)	Copy %	Share Ready
mp3	true	Share Ready, Sync Enabled. Last successful sync time : Mon Jun 27 15:37:12 2005 Last sync : Success	38	100	true
sh1	true	Share Ready, Sync Disabled. Last successful sync time : Wed Jun 15 16:43:52 2005 Last sync : Success	221	100	true
sh2	true	Share Ready, Sync Enabled. Last successful sync time : Mon Jun 27 15:37:57 2005 Last sync : Success	0	100	true
sh3	true	Share Ready, Sync Enabled. Last successful sync time : Mon Jun 27 15:31:11 2005 Last sync : Success	54	100	true
sh4	true	Share Ready, Sync Enabled. Last successful sync time : Mon Jun 27 15:37:23 2005 Last sync : Success	21	100	true

**Performance**

- Bandwidth Optimization
- Data Store Hit Rate
- Data Reduction
- NFS Statistics
- Throughput
- Traffic Summary

**Appliance**

- Data Store
- TCP Statistics

**Network**

- Connected Appliances
- Connection History
- Current Connections
- Connection Pooling
- Interface Statistics
- Link State Statistics
- Neighbor Statistics
- QoS Statistics

**Health**

- Alarm Status
- CPU Utilization
- Memory Paging

**Proxy File Service**

- **Share Status** «
- Statistics

**Export**

- Statistics

**Diagnostic**

- System Dumps
- System Snapshots
- TCP Dumps

**TIP:** Click the local name to display the PFS - Shares page.

## Viewing PFS Statistics

The PFS Statistics report summarizes PFS connection statistics for the time period specified.

The PFS Statistics report contains the following table of statistics that summarize PFS activity.

Packet Type	Description
Bytes Received	Specifies the total bytes received on the specified share.
Peak Bytes Received Over Last Month	Specifies the peak number of bytes received over the last month on the specified share.
Peak Bytes Occurred At	Specifies the date and time for the peak activity for the share.
Bytes Sent	Specifies the total bytes sent for the specified share.
Peak Bytes Sent Over Last Month	Specifies the peak number of bytes sent over the last month on the specified share.
Peak Bytes Sent Occurred At	Specifies the date and time for the peak bytes sent for the share.

## What this Report Tells You

The PFS Statistics report answers the following questions:

- ◆ How many bytes were sent and received for the specified share?
- ◆ How many bytes were sent and received over the last month for the specified share?
- ◆ What is the date and time for the peak activity (both, sent and received)?

## About Report Graphs

In bar-graph and line-graph reports, the *x*-axis (or tick mark) plots time, according to the interval you select. The *y*-axis plots the metric of interest, such as gigabytes (GB) of bandwidth, percent (%) of data reduction, connection counts, and the like.

A diamond icon above the top margin of the graph points to the value on the *x*-axis (the time) at which the peak occurred.

A diamond icon outside the right margin of the graph points to the value on the *y*-axis (for example, the percent) that is the average value for the time period selected.

Pie chart graphs do not indicate peaks or averages. Pie chart graphs represent the aggregate for the time period selected.

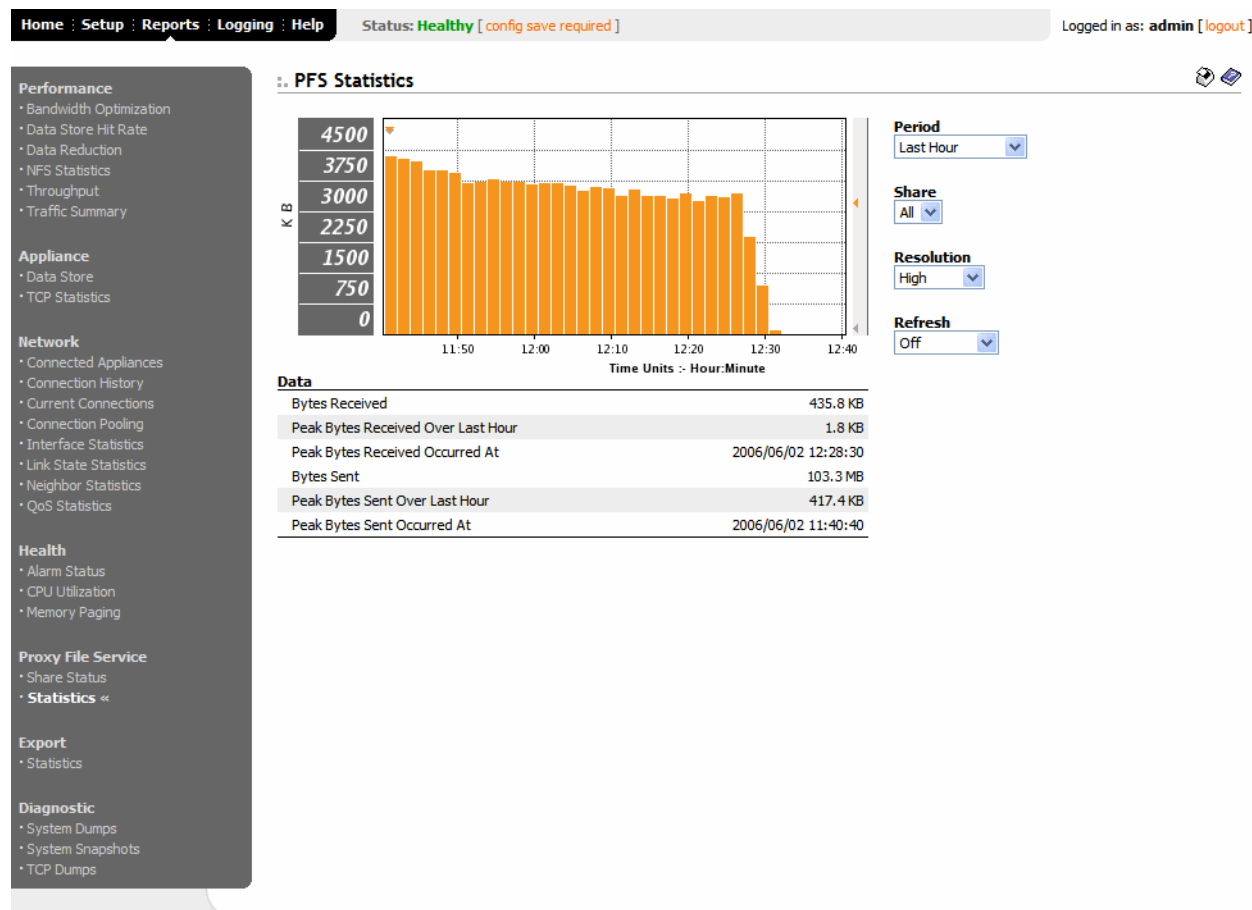
## About Report Data

The HP EFS WAN Accelerator system polls bandwidth and connection metrics every second and can report on performance for periods as long as one year. However, due to performance and disk space considerations, data representation in reports for periods longer than the Last 5 Minutes are interpolated from aggregate data points.

## To view the PFS Share: Name-of-Share report

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Click Statistics in the left menu to display the PFS Statistics page.

**Figure 3-22. PFS Statistics Page**



3. Use the controls to customize the report, as described in the following table..

Control	Description
Period	Select <b>Last Hour</b> , <b>Last Day</b> , <b>Last Week</b> , or <b>Last Month</b> from the drop-down list.
Share	Select <b>All</b> or a specific share from the drop-down list.
Resolution	Select <b>High</b> , <b>Medium</b> , or <b>Low</b> from the <b>Resolution</b> drop-down list. <b>High</b> (small bars) allows you to drill down to specific points in time, while <b>Low</b> (large bars) enables you to count or compare aggregate values in the time interval.
Refresh	Set a rate to refresh the report display: <ul style="list-style-type: none"> <li>• To refresh your report every 15 seconds, click <b>15 Seconds</b>.</li> <li>• To refresh your report every 30 seconds, click <b>30 Seconds</b>.</li> <li>• To turn off refresh, click <b>Off</b>.</li> </ul> <b>NOTE:</b> The refresh rate does not affect polling. Polling occurs every 5 minutes.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Exporting Performance Statistics

# Exporting Performance Statistics Reports

The following section describes how to export performance statistics reports.

You can export performance statistics in comma-separated value (CSV) format in the Export - Statistics report. The CSV format allows you to easily import the statistics into spreadsheets and databases. You can open the CSV file in any text editor.

The CSV file contains commented lines (comments beginning with the # character) at the beginning of the file. These comments report what host generated the file, the report that was generated, time boundaries, the time the export occurred, and the version of the HP EFS WAN Accelerator the file was exported from. The statistical values are provided in columns: the first column is the date and time of the statistic sample, the columns that follow contain the data.

### To export statistics

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Export in the left menu, click Statistics to display the Export - Statistics page.

**Figure 3-23. Export - Statistics Page**

The screenshot shows the HP EFS WAN Accelerator web interface. At the top, there is a navigation bar with links: Home, Setup, Reports, Logging, and Help. The Reports link is highlighted. To the right of the navigation bar, the status is shown as 'Healthy' with a note '[ config save required ]', and the user is logged in as 'admin' with a '[ logout ]' link.

On the left side, there is a sidebar menu with categories: Performance, Appliance, Network, Health, Proxy File Service, Export, and Diagnostic. The 'Export' category is expanded, showing 'Statistics' as the selected option.

The main content area is titled 'Export Statistics'. Below the title, there is a message: 'Select a report you want to export and optionally enter cut-off dates for the export.' Below this message is a form with the following fields:

- Report:** A dropdown menu with 'cpu\_util (CPU utilization)' selected.
- After:** A text input field with a placeholder '(optional YYYY/MM/DD HH:MM:SS)'.
- Before:** A text input field with a placeholder '(optional YYYY/MM/DD HH:MM:SS)'.
- Export:** A button to submit the form.

3. Use the controls to customize the report, as described in the following table..

Control	Description
Report	Select the report you want to export from the drop-down list.
After	Specify a date and time from which the statistics should begin in the After text box. Use the following format: <b>YYYY/MM/DD HH:MM:SS</b> .
Before	Specify a date and time from which the statistics should begin in the After text box. Use the following format: <b>YYYY/MM/DD HH:MM:SS</b>
Export	Click <b>Export</b> to export your data.
Printer icon	To print your report, click the <b>Printer</b> icon in the upper right corner of the page.

## Viewing System Diagnostic Files

The following section describes how to view HP EFS WAN Accelerator system files to help diagnose problems. It includes the following sections:

- ◆ [“Viewing System Dump Files,”](#) next
- ◆ [“Viewing System Snapshots”](#) on page 198
- ◆ [“Viewing TCP Dump Files”](#) on page 199

### Viewing System Dump Files

The Diagnostic - System Dump Report displays a list of system dump files and their size. A system dump contains a copy of the kernel data on the system. System dump files can help you diagnose problems in the HP EFS WAN Accelerator.

## To view system dump files

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Diagnostic in the left menu, click System Dumps to display the Diagnostic - System Dumps page.

**Figure 3-24. Diagnostic - System Dumps Page**

The screenshot displays the 'System Dumps' page. The top navigation bar includes 'Home', 'Setup', 'Reports', 'Logging', and 'Help'. The status is 'Healthy', and the user is logged in as 'admin'. The left sidebar shows a menu with categories: Performance, Appliance, Network, Health, Proxy File Service, Export, and Diagnostic. Under 'Diagnostic', 'System Dumps' is selected. The main content area is titled 'System Dumps' and contains a message: 'The following is a list of diagnostic system dumps stored on the appliance.' Below this is a table with two columns: 'Name' and 'Size'. The table lists five files, each with a checkbox for selection. Below the table, there is a 'Remove Selected Files' button and a 'Generate System Dump Now' button.

Name	Size
<input type="checkbox"/> evsdump-gen-sh87-20060606-100447.tgz	612454 bytes
<input type="checkbox"/> sysdump-gen-sh87-20060606-101139.tgz	611465 bytes
<input type="checkbox"/> sysdump-gen-sh87-20060606-102412.tgz	615758 bytes
<input type="checkbox"/> sysdump-gen-sh87-20060606-110314.tgz	635525 bytes
<input type="checkbox"/> sysdump-gen-sh87-20060606-113227.tgz	606529 bytes

5 file(s)

[Remove Selected Files](#)

[Generate System Dump Now](#)

3. Click the file name to open a file save dialog box to download the file.
4. Click **Generate System Dump Now** to generate a new system dump.

**TIP:** To remove an entry, click the check box next to the name and click **Remove Selected Files**. This action applies the settings to the running configuration. Click **Save** to write your settings to memory or click **Reset** to return the settings to their previous values.

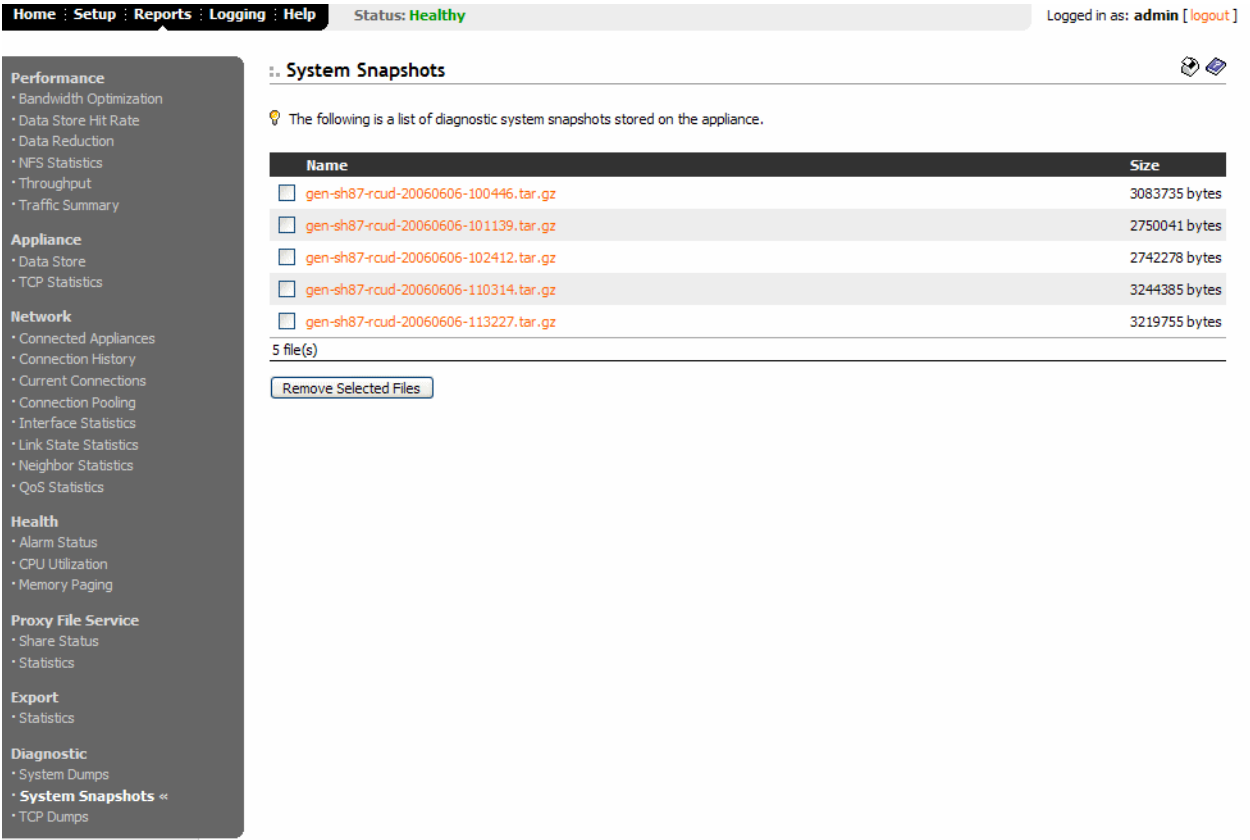
## Viewing System Snapshots

The Diagnostic -System Snapshots report displays a list of system snapshot files and their size. A system snapshot is a saved copy of memory including the contents of all memory, bytes, hardware registers, and status indicators. It is periodically taken to restore the system in the event of failure. System snapshot files can help you diagnose problems in the HP EFS WAN Accelerator.

### To view system snapshot files

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Diagnostic in the left menu, click System Snapshots to display the Diagnostic - System Snapshots page.

Figure 3-25. Diagnostic - System Snapshots Page



3. Click the file name to open a file save dialog box to download the file.

---

**TIP:** To remove an entry, click the check box next to the name and click **Remove Selected Files**.

---

### Viewing TCP Dump Files

The Diagnostic -TCP Dumps report displays a list of system snapshot files and their size. TCP dump files contain summary information for every Internet packet received or transmitted on the interface. TCP dump files can help you diagnose problems in the HP EFS WAN Accelerator.

To view TCP data you must run the **tcpdump** tool using the HP EFS WAN Accelerator CLI. For detailed information, see the *HP StorageWorks Enterprise File Services WAN Accelerator Command Line Interface Reference Manual*.

## To view TCP dump files

1. Click the Reports tab to display the Performance - Bandwidth Optimization page.
2. Under Diagnostic in the left menu, click TCP Dump to display the Diagnostic - TCP Dump page.

**Figure 3-26. Diagnostic - TCP Dump Page**

The screenshot shows the HP EFS WAN Accelerator web interface. At the top, there is a navigation bar with tabs: Home, Setup, Reports, Logging, and Help. The 'Reports' tab is selected. To the right of the tabs, the status is 'Healthy' with a note '[ config save required ]'. Further right, it says 'Logged in as: admin [logout]'. On the left side, there is a dark sidebar menu with categories: Performance (Bandwidth Optimization, Data Store Hit Rate, Data Reduction, NFS Statistics, Throughput, Traffic Summary), Appliance (Data Store, TCP Statistics), Network (Connected Appliances, Connection History, Current Connections, Connection Pooling, Interface Statistics, Link State Statistics, Neighbor Statistics, QoS Statistics), Health (Alarm Status, CPU Utilization, Memory Paging), Proxy File Service (Share Status, Statistics), Export (Statistics), and Diagnostic (System Dumps, System Snapshots, TCP Dumps <<). The 'TCP Dumps' item is highlighted. The main content area is titled 'TCP Dumps' and contains a message: 'The following is a list of diagnostic TCP dumps stored on the appliance.' Below this is a table with columns 'Name' and 'Size'. The table is currently empty, showing 'No files.' Below the table is a button labeled 'Remove Selected Files'.

3. Click the file name to open a file save dialog box to download the file.

---

**TIP:** To remove an entry, click the check box next to the name and click **Remove Selected Files**.

---

## Viewing HP EFS WAN Accelerator Logs

The following section describes how to view HP EFS WAN Accelerator logs.



## Viewing HP EFS WAN Accelerator Logs

You can view HP EFS WAN Accelerator logs in the Logging: System Log report. Use system logs to monitor HP EFS WAN Accelerator activity and to troubleshoot problems with the system. The most recent log events are listed first.

### To view HP EFS WAN Accelerator logs

1. Click the Logging tab to display the Logging: System Log page.

**Figure 3-27. Logging: Current Log Page**

The screenshot shows the HP EFS WAN Accelerator Management Console interface. At the top, a navigation bar includes links for Home, Setup, Reports, Logging, and Help. The status is 'Healthy' with a note 'config save required'. The user is logged in as 'admin'. The left sidebar contains a 'Current Log' section with a list of archived logs (1-10) and a 'Launch Continuous Log' button. The main content area is titled 'System Log' and features a 'Filter' input field. Below this, there are navigation links for 'Prev' and 'Next', and a 'Page' selector showing 'Page: 1 2 3 4 5 ... 924 925 926 927 [928]'. The log events are listed in a table with columns for time, source, and message. The events show various system activities, including session openings and data transfers. At the bottom, there is a 'Jump to Page' field with a 'Go' button.

2. Use the controls to customize your logs, as described in the following table.

Control	Description
Filter	Specify a keyword or string and click <b>Filter</b> to display logs according to the parameters you specify.
Prev	Click <b>Prev</b> to view previous pages in the log.
Page #	Click the page number to view additional pages in the log.
Jump to Page	Specify a page number and click <b>Go</b> to view the log page you specified.
Launch Continuous Log	Click <b>Launch Continuous Log</b> to display continuous log messages in your Web browser. (This feature might not be supported in all Web browsers.)
Rotate Logs Now	Click <b>Rotate Logs Now</b> to archive the current log.
Disk Icon	Click the <b>Disk</b> icon in the upper right corner to download the log file to your local machine.

---

## Getting Help

The following section describes how to obtain help with your HP EFS WAN Accelerator. It includes the following sections:

- ◆ [“Contacting Technical Support,”](#) next
- ◆ [“Viewing Online Help Contents”](#) on page 202

### Contacting Technical Support

You can obtain the technical support phone number from the Help: Technical Support page.

---

**TIP:** Under Website, click the Web site link to go to the HP technical support Web site.

---

### Viewing Online Help Contents

#### To view online help contents

You can view the table of contents for online help in the Help: Online Help page. The online help contains page-level help for each page in the Management Console.

1. Click the Help tab to display the Help: Technical Support page.
2. Click Online Help in the left menu to display the Help: Online Help page.
3. Click the **Click here for online help** link to display the online help table of contents.

## APPENDIX A

# HP EFS WAN Accelerator Ports

## In This Appendix

This appendix describes the HP EFS WAN Accelerator default and supported secure ports. It includes the following sections:

- ◆ [“Default Ports,”](#) next
- ◆ [“Commonly Optimized Ports”](#) on page 204
- ◆ [“Commonly Excluded Ports”](#) on page 204
- ◆ [“Interactive Ports Forwarded by the HP EFS WAN Accelerator”](#) on page 205
- ◆ [“Secure Ports Forwarded by the HP EFS WAN Accelerator”](#) on page 206

---

## Default Ports

The following table summarizes HP EFS WAN Accelerator default ports with the port label: RBT-Proto.

Default Ports	Description
7744	Data store synchronization port.
7800	In-path port for appliance to appliance connections.
7801	Network Address Translation (NAT) port.
7810	Out-of-path server port.
7820	Failover port for redundant appliances.
7830	Messaging Application Programming Interface (MAPI) Exchange 2003 port.
7840	Name Service Provider Interface (NSPI) port.
7850	Connection forwarding (neighbor) port.
7860	Interceptor appliance

---

**IMPORTANT:** For two HP EFS WAN Accelerators to optimize traffic, ports **7800** and **7810**, must be passed through firewall devices located between the pair of HP EFS WAN Accelerators. Also, SYN and SYN/ACK packets with the TCP option **76** must be passed through firewalls for autodiscovery to function properly. For the HP EFS WAN Accelerator Manager, port **22** must be passed through the firewall for it to function properly.

---

---

## Commonly Optimized Ports

The HP EFS WAN Accelerator by default optimizes all ports. If you do not want the HP EFS WAN Accelerator to optimize all ports for an in-path or out-of path configuration, you can specify specific ports for optimization.

Although these ports can vary according to your requirements, the following ports are commonly optimized and monitored for in-path and out-of-path configurations:

- ◆ 21 (FTP)
- ◆ 49 (TACACS+)
- ◆ 80 (HTTP)
- ◆ 139 (CIFS:NETBIOS)
- ◆ 445 (CIFS:TCP)
- ◆ 1433 (SQL:TDS)
- ◆ 1812 (Radius)
- ◆ 7830 (MAPI)

---

## Commonly Excluded Ports

This section summarizes the ports that are commonly excluded from optimization in the HP EFS WAN Accelerator.

If you have multiple ports that you want to exclude, create a port label and list the ports.

Application	Ports
PolyComm (video conferencing)	1503, 1720-1727, 3230-3253, 5060
Cisco IPTel	2000

## Interactive Ports Forwarded by the HP EFS WAN Accelerator

A default in-path rule with the port label **Interactive** is automatically created in your system. This in-path rule automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell).

**TIP:** If you do not want to automatically forward these ports, simply delete the **Interactive** rule in the Management Console.

The following table lists the interactive ports that are automatically forwarded by the HP EFS WAN Accelerator.

Port	Description
7	TCP ECHO
23	Telnet
37	UDP/Time
107	Remote Telnet Service
179	Border Gateway Protocol
513	Remote Login
514	Shell
1494	Citrix
1718-1720	h323gatedisc
2000-2003	Cisco SCCp
2427	Media Gateway Control Protocol Gateway
2598	Citrix
2727	Media Gateway Control Protocol Call Agent
3389	MS WBT Server, TS/Remote Desktop
5060	SIP
5631	PC Anywhere
5900-5903	VNC
6000	X11

---

## Secure Ports Forwarded by the HP EFS WAN Accelerator

A default in-path rule with the port label **Secure** is automatically created in your system. This in-path rule automatically passes through traffic on commonly secure ports (for example, **ssh**, **https**, and **smtps**).

---

**TIP:** If you do not want to automatically forward these ports, simply delete the **Secure** rule in the Management Console.

---

The following table lists the common secure ports that are automatically forwarded by the HP EFS WAN Accelerator.

Type	Port	Description
ssh	22/tcp	SSH Remote Login Protocol
tacacs	49/tcp	TACACS+
https	443/tcp	http protocol over TLS/SSL
smtps	465/tcp	# SMTP over SSL (TLS)
nntp	563/tcp	nntp protocol over TLS/SSL (was snntp)
imap4-ssl	585/tcp	IMAP4+SSL (use 993 instead)
sshell	614/tcp	SSLshell
ldaps	636/tcp	ldap protocol over TLS/SSL (was sldap)
ftps-data	989/tcp	ftp protocol, data, over TLS/SSL
ftps	990/tcp	ftp protocol, control, over TLS/SSL
telnet	992/tcp	telnet protocol over TLS/SSL
imaps	993/tcp	imap4 protocol over TLS/SSL
pop3s	995/tcp	pop3 protocol over TLS/SSL (was spop3)
l2tp	1701/tcp	l2tp
pptp	1723/tcp	pptp
tftps	3713/tcp	TFTP over TLS

The following table contains the uncommon ports automatically forwarded by the HP EFS WAN Accelerator.

Type	Port	Description
nsiiops	261/tcp	IIOP Name Service over TLS/SSL
ddm-ssl	448/tcp	DDM-Remote DB Access Using Secure Sockets
corba-iiop-ssl	684/tcp	CORBA IIOP SSL
ieee-mms-ssl	695/tcp	IEEE-MMS-SSL
ircs	994/tcp	irc protocol over TLS/SSL
njenet-ssl	2252/tcp	NJENET using SSL
ssm-cssps	2478/tcp	SecurSight Authentication Server (SSL)
ssm-els	2479/tcp	SecurSight Event Logging Server (SSL)
giop-ssl	2482/tcp	Oracle GIOP SSL
ttc-ssl	2484/tcp	Oracle TTC SSL
syncserverssl	2679/tcp	Sync Server SSL
dicom-tls	2762/tcp	DICOM TLS
realsecure	2998/tcp	Real Secure
orbix-loc-ssl	3077/tcp	Orbix 2000 Locator SSL
orbix-cfg-ssl	3078/tcp	Orbix 2000 Locator SSL
cops-tls	3183/tcp	COPS/TLS
csvr-sslproxy	3191/tcp	ConServR SSL Proxy
xnm-ssl	3220/tcp	XML NM over SSL
msft-gc-ssl	3269/tcp	Microsoft Global Catalog with LDAP/SSL
networklenss	3410/tcp	NetworkLens SSL Event
xtrms	3424/tcp	xTrade over TLS/SSL
jt400-ssl	3471/tcp	jt400-ssl
seclayer-tls	3496/tcp	securitylayer over tls
vt-ssl	3509/tcp	Virtual Token SSL Port
jboss-iiop-ssl	3529/tcp	JBoss IIOP/SSL
ibm-diradm-ssl	3539/tcp	IBM Directory Server SSL
can-nds-ssl	3660/tcp	Candle Directory Services using SSL
can-ferret-ssl	3661/tcp	Candle Directory Services using SSL
linktest-s	3747/tcp	LXPRO.COM LinkTest SSL
asap-tcp-tls	3864/tcp	asap/tls tcp port
topflow-ssl	3885/tcp	TopFlow SSL
sdo-tls	3896/tcp	Simple Distributed Objects over TLS

Type	Port	Description
sdo-ssh	3897/tcp	Simple Distributed Objects over SSH
iss-mgmt-ssl	3995/tcp	ISS Management Svcs SSL
suucp	4031/tcp	UUCP over SSL
wsm-server-ssl	5007/tcp	wsm server ssl
sip-tls	5061/tcp	SIP-TLS
imqtunnels	7674/tcp	iMQ SSL tunnel
davsrce	9802/tcp	WebDAV Source TLS/SSL
intrepid-ssl	11751/tcp	Intrepid SSL
rets-ssl	12109/tcp	RETS over SSL



## APPENDIX B

# HP EFS WAN Accelerator MIB

## In This Appendix

This appendix describes the HP EFS WAN Accelerator Enterprise Simple Network Management Protocol (SNMP) Message Information Base (MIB). It includes the following sections:

- ◆ “Accessing the HP EFS WAN Accelerator Enterprise MIB,” next
- ◆ “HP EFS WAN Accelerator Enterprise MIB” on page 211

---

## Accessing the HP EFS WAN Accelerator Enterprise MIB

The HP EFS WAN Accelerator Enterprise MIB monitors device status, peers, and provides network statistics for seamless integration into network management systems such as Hewlett Packard OpenView Network Node Manager, Paessler Router Traffic Grapher (PRTG), and other SNMP browser tools.

For detailed information about configuring and using these network monitoring tools, consult their individual web sites.

The following guidelines describe how to download and access the HP EFS WAN Accelerator Enterprise MIB using common MIB browsing utilities.

- ◆ You can download the HP EFS WAN Accelerator Enterprise MIB (**RBT-mib.txt**) from the HP support site at <http://www.hp.com> and load it into any MIB browser utility.
- ◆ Some utilities might expect a file type other than a text file. If this occurs, change the file type to the one expected.
- ◆ Some utilities assume that the root is **mib-2** by default. If the utility sees a new node, such as **enterprises**, it might look under **mib-2.enterprises**. If this occurs, use **.iso.org.dod.internet.private.enterprises.rbt** as the root.
- ◆ Some command-line browsers might not load all MIB files by default. If this occurs, find the appropriate command option to load the **RBT-mib.txt** file. For example, for NET-SNMP browsers: **snmwalk -m all**

---

## SNMP Traps

The following table summarizes the Simple Network Management Protocol (SNMP) traps sent out from the HP EFS WAN Accelerator to configured trap receivers.

Trap	Description
procCrash (enterprises.17163.1.1.4.1)	A process has crashed and subsequently been restarted by the system. A system snapshot associated with this crash has been created on the HP EFS WAN Accelerator and is accessible via the CLI or Management Console. HP Technical Support may need this information to determine the cause of the crash.
procExit (enterprises.17163.1.1.4.2)	A process has unexpectedly exited and been restarted by the system. The process may have exited on its own or due to other process failures on the HP EFS WAN Accelerator. Please contact HP Technical Support to determine the cause of this event.
cpuUtil (enterprises.17163.1.1.4.3)	Average CPU utilization has exceeded an acceptable threshold. If CPU utilization spikes are frequent, it may be because the system is undersized. Sustained CPU load may be symptomatic of more serious issues; please contact HP Technical Support for more information.
pagingActivity (enterprises.17163.1.1.4.4)	The system is running low on memory and has begun swapping memory pages to disk. This event can be triggered during a software upgrade on an optimizing HP EFS WAN Accelerator and is normal. Should this event be triggered at any other time, please contact HP Technical Support.
smartError (enterprises.17163.1.1.4.5)	A disk is about to fail. Contact HP Technical Support immediately.  <b>NOTE:</b> Applicable to models 510, 520, 1010, 1020, 2010, 2020 only.
peerVersionMismatch (enterprises.17163.1.1.4.6)	The HP EFS WAN Accelerator has encountered another HP EFS WAN Accelerator which is running an incompatible version of system software. The CLI, Management Console, or the SNMP peer table can be referenced to determine which HP EFS WAN Accelerator is causing the conflict. To resolve the problem: upgrade your system software.
bypassMode (enterprises.17163.1.1.4.7)	The HP EFS WAN Accelerator has entered bypass mode and is now passing through all traffic unoptimized. This event can be the result of a system crash or a manual configuration change, such as a service restart or system reboot.
raidError (enterprises.17163.1.1.4.8)	A drive has failed in a RAID array. Consult the CLI or Management Console to determine the location of the failed drive. Please contact HP Technical Support for assistance with installing the spare drive. The appliance will continue to optimize during this event.  <b>NOTE:</b> Applicable to models 3010 and 5010 only.
storeCorruption (enterprises.17163.1.1.4.9)	Corruption has been detected in the data store. Please contact HP Technical Support immediately

Trap	Description
admissionMemError (enterprises.17163.1.1.4.10)	The HP EFS WAN Accelerator is optimizing traffic beyond its rated capability. During this event, the HP EFS WAN Accelerator will continue to optimize existing connections, but new connections will be passed through without optimization.
admissionConnError (enterprises.17163.1.1.4.11)	The HP EFS WAN Accelerator is optimizing a number of connections beyond its rated capability. During this event, the HP EFS WAN Accelerator will continue to optimize existing connections, but new connections will be passed through without optimization.
haltError (enterprises.17163.1.1.4.12)	The optimization service has halted due to a serious software error. Please contact HP Technical Support immediately.
serviceError (enterprises.17163.1.1.4.13)	The optimization service has encountered a condition which may degrade optimization performance. Please consult the system log for more information.
scheduledJobError (enterprises.17163.1.1.4.14)	A scheduled job on the system (e.g., a software upgrade) has failed. Please use the CLI or the Management Console to determine which job failed.
confModeEnter (enterprises.17163.1.1.4.15)	A user on the system has entered configuration mode from either the CLI or Management Console.
confModeExit (enterprises.17163.1.1.4.16)	A user on the system has entered configuration mode from either the CLI or Management Console.

## HP EFS WAN Accelerator Enterprise MIB

The following text is an example of the HP EFS WAN Accelerator Enterprise MIB file (**RBT-mib.txt**).

```
STEELHEAD-MIB DEFINITIONS ::= BEGIN

IMPORTS
    OBJECT-TYPE, MODULE-IDENTITY, NOTIFICATION-TYPE, enterprises,
    Unsigned32,
        TimeTicks, IpAddress, Counter64 FROM SNMPv2-SMI
    DateAndTime FROM SNMPv2-TC
    products FROM RBT-MIB;

steelhead MODULE-IDENTITY
    LAST-UPDATED          "200608040000Z"
    ORGANIZATION          "Riverbed Technology, Inc."
    CONTACT-INFO
        "    Balaji Ramachandran
        balajir@riverbed.com"
    DESCRIPTION           "Steelhead MIB"
    ::= { products 1 }

system OBJECT IDENTIFIER
    ::= { steelhead 1 }

status OBJECT IDENTIFIER
    ::= { steelhead 2 }
```

```

config OBJECT IDENTIFIER
    ::= { steelhead 3 }

alarms OBJECT IDENTIFIER
    ::= { steelhead 4 }

statistics OBJECT IDENTIFIER
    ::= { steelhead 5 }

--
--
-- SYSTEM
--
--

model OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Appliance model"
    ::= { system 1 }

serialNumber OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Appliance serial number"
    ::= { system 2 }

systemVersion OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "System software version string"
    ::= { system 3 }

--
--
-- STATUS
--
--

systemClock OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "System clock time"
    ::= { status 1 }

health OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current health"
    ::= { status 2 }

serviceStatus OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only

```

```

        STATUS          current
        DESCRIPTION
            "Current service status"
        ::= { status 3 }

serviceUptime OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current service uptime"
    ::= { status 4 }

procTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF ProcEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "List of managed processes"
    ::= { status 5 }

procEntry OBJECT-TYPE
    SYNTAX      ProcEntry
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Entry for one process"
    INDEX       { procIndex }
    ::= { procTable 1 }

ProcEntry ::=
    SEQUENCE {
        procIndex          Unsigned32,
        procName           OCTET STRING,
        procStatus         OCTET STRING,
        procNumFailures    Unsigned32
    }

procIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION
        "Synthetic numeric unique ID of process"
    ::= { procEntry 1 }

procName OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Unique name of process"
    ::= { procEntry 2 }

procStatus OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current state of process"
    ::= { procEntry 3 }

procNumFailures OBJECT-TYPE
    SYNTAX      Unsigned32

```

```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Number of times process has crashed or exited unexpectedly"
::= { procEntry 4 }

peerStatus OBJECT IDENTIFIER
::= { status 6 }

peerTable OBJECT-TYPE
SYNTAX SEQUENCE OF PeerEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "List of peers"
::= { peerStatus 1 }

peerEntry OBJECT-TYPE
SYNTAX PeerEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "Entry for one peer"
INDEX { peerIndex }
::= { peerTable 1 }

PeerEntry ::=
SEQUENCE {
    peerIndex Unsigned32,
    peerHostname OCTET STRING,
    peerVersion OCTET STRING,
    peerAddress IpAddress,
    peerModel OCTET STRING
}

peerIndex OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
    "Index of peer"
::= { peerEntry 1 }

peerHostname OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Hostname of peer"
::= { peerEntry 2 }

peerVersion OBJECT-TYPE
SYNTAX OCTET STRING
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "System software version of peer"
::= { peerEntry 3 }

peerAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
DESCRIPTION

```

```

        "IP address of peer"
        ::= { peerEntry 4 }

peerModel OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Model of peer"
        ::= { peerEntry 5 }

--
--
-- CONFIG
--
--

activeConfig OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current active configuration"
        ::= { config 1 }

inpath OBJECT IDENTIFIER
    ::= { config 2 }

inpathSupport OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "In-path support"
        ::= { inpath 1 }

outofpath OBJECT IDENTIFIER
    ::= { config 3 }

outofpathSupport OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Out-of-path support"
        ::= { outofpath 1 }

--
--
-- ALARMS
--
--

alarmsPrefix OBJECT IDENTIFIER
    ::= { alarms 0 }

procCrash NOTIFICATION-TYPE
    OBJECTS { procName }
    STATUS      current
    DESCRIPTION
        "A procCrash trap signifies that a process managed by PM
        has crashed and left a core file. The variable sent with
        the notification indicates which process crashed."
        ::= { alarmsPrefix 1 }

```

```

procExit NOTIFICATION-TYPE
  OBJECTS { procName }
  STATUS  current
  DESCRIPTION
    "A procExit trap signifies that a process managed by PM
    has exited unexpectedly, but not left a core file.
    The variable sent with the notification indicates
    which process exited."
  ::= { alarmsPrefix 2 }

cpuUtil NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "The average CPU utilization in the past minute has gone
    above the acceptable threshold"
  ::= { alarmsPrefix 3 }

pagingActivity NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "The system has been paging excessively (thrashing)"
  ::= { alarmsPrefix 4 }

smartError NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "SMART has sent an event about a possible disk error"
  ::= { alarmsPrefix 5 }

peerVersionMismatch NOTIFICATION-TYPE
  OBJECTS { systemVersion }
  STATUS  current
  DESCRIPTION
    "Detected a peer with a mismatched software version"
  ::= { alarmsPrefix 6 }

bypassMode NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "The appliance has entered bypass (failthru) mode"
  ::= { alarmsPrefix 7 }

raidError NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "An error has been generated by the RAID array"
  ::= { alarmsPrefix 8 }

storeCorruption NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "The data store is corrupted"
  ::= { alarmsPrefix 9 }

admissionMemError NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION
    "Admission control memory alarm has been triggered"
  ::= { alarmsPrefix 10 }

admissionConnError NOTIFICATION-TYPE
  STATUS  current
  DESCRIPTION

```



```

        "Admission control connections alarm has been triggered"
        ::= { alarmsPrefix 11 }

haltError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "The service is halted due to a software error"
        ::= { alarmsPrefix 12 }

serviceError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "There has been a service error. Please consult the log file"
        ::= { alarmsPrefix 13 }

scheduledJobError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "A scheduled job has failed during execution"
        ::= { alarmsPrefix 14 }

confModeEnter NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "A user has entered configuration mode"
        ::= { alarmsPrefix 15 }

confModeExit NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "A user has exited configuration mode"
        ::= { alarmsPrefix 16 }

linkError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "An interface has lost link on the appliance"
        ::= { alarmsPrefix 17 }

nfsV2V4 NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "NFS v2/v4 alarm notification"
        ::= { alarmsPrefix 18 }

powerSupplyError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "A power supply on the appliance has failed. Not supported
on all models"
        ::= { alarmsPrefix 19 }

asymRouteError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "Asymmetric routes have been detected,certain connections
might
not have been optimized because of this."
        ::= { alarmsPrefix 20 }

fanError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION

```

```

        "A fan error has been detected on the appliance. Not
supported on all models"
        ::= { alarmsPrefix 21 }

memoryError NOTIFICATION-TYPE
    STATUS current
    DESCRIPTION
        "A memory error has been detected on the appliance. Not
supported on all models"
        ::= { alarmsPrefix 22 }

--
--
-- STATISTICS
--
--

cpuLoad OBJECT IDENTIFIER
    ::= { statistics 1 }

cpuLoad1 OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "One-minute CPU load in hundreths"
    ::= { cpuLoad 1 }

cpuLoad5 OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Five-minute CPU load in hundreths"
    ::= { cpuLoad 2 }

cpuLoad15 OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Fifteen-minute CPU load in hundreths"
    ::= { cpuLoad 3 }

cpuUtil1 OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Percentage CPU utilization, aggregated across all CPUs, rolling
        average over the past minute"
    ::= { cpuLoad 4 }

cpuIndivUtilTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CPUIndivUtilEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Details about the individual CPU utilization"
    ::= { cpuLoad 5 }

cpuIndivUtilEntry OBJECT-TYPE
    SYNTAX      CPUIndivUtilEntry
    MAX-ACCESS  not-accessible

```

```

        STATUS      current
        DESCRIPTION
            "Entry for one cpu"
        INDEX      { cpuIndivId }
        ::= { cpuIndivUtilTable 1 }

CPUIndivUtilEntry ::=
    SEQUENCE {
        cpuIndivIndex      Unsigned32,
        cpuIndivId         Unsigned32,
        cpuIndivIdleTime   Unsigned32,
        cpuIndivSystemTime Unsigned32,
        cpuIndivUserTime   Unsigned32
    }

cpuIndivIndex OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index for the table"
    ::= { cpuIndivUtilEntry 1 }

cpuIndivId OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index for the table"
    ::= { cpuIndivUtilEntry 2 }

cpuIndivIdleTime OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Idle time for this CPU"
    ::= { cpuIndivUtilEntry 3 }

cpuIndivSystemTime OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "System time for this CPU"
    ::= { cpuIndivUtilEntry 4 }

cpuIndivUserTime OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "User time for this CPU"
    ::= { cpuIndivUtilEntry 5 }

connectionCounts OBJECT IDENTIFIER
    ::= { statistics 2 }

optimizedConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Current total number of optimized connections"

```

```

        ::= { connectionCounts 1 }

passthroughConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current total number of pass-through connections"
    ::= { connectionCounts 2 }

halfOpenedConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current total number of half-opened (optimized) connections"
    ::= { connectionCounts 3 }

halfClosedConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current total number of half-closed (optimized) connections"
    ::= { connectionCounts 4 }

establishedConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current number of established (optimized) connections"
    ::= { connectionCounts 5 }

activeConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Current number of active (optimized) connections"
    ::= { connectionCounts 6 }

totalConnections OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Total number of connections"
    ::= { connectionCounts 7 }

bandwidth OBJECT IDENTIFIER
    ::= { statistics 3 }

bandwidthAggregate OBJECT IDENTIFIER
    ::= { bandwidth 1 }

bwAggInLan OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
        "Total bytes WanToLan LAN side since last restart of service"
    ::= { bandwidthAggregate 1 }

```

```

bwAggInWan OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total bytes WanToLan WAN side since last restart of service"
    ::= { bandwidthAggregate 2 }

bwAggOutLan OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total bytes LanToWan LAN side since last restart of service"
    ::= { bandwidthAggregate 3 }

bwAggOutWan OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Total bytes LanToWan WAN side since last restart of service"
    ::= { bandwidthAggregate 4 }

bandwidthPerPort OBJECT IDENTIFIER
    ::= { bandwidth 2 }

bwPortTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF BWPortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "List of bandwidth ports"
    ::= { bandwidthPerPort 1 }

bwPortEntry OBJECT-TYPE
    SYNTAX      BWPortEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Entry for one port"
    INDEX      { bwPort }
    ::= { bwPortTable 1 }

BWPortEntry ::=
    SEQUENCE {
        bwPort                Unsigned32,
        bwPortInLan           Counter32,
        bwPortInWan           Counter32,
        bwPortOutLan          Counter32,
        bwPortOutWan          Counter32,
        bwPortNumber          Unsigned32
    }

bwPort OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Index for the table"
    ::= { bwPortEntry 1 }

bwPortInLan OBJECT-TYPE
    SYNTAX      Counter32

```

```

MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Bytes WanToLan LAN side since last restart of service"
::= { bwPortEntry 2 }

bwPortInWan OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Bytes WanToLan WAN side since last restart of service"
::= { bwPortEntry 3 }

bwPortOutLan OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Bytes LanToWan LAN side since last restart of service"
::= { bwPortEntry 4 }

bwPortOutWan OBJECT-TYPE
SYNTAX Counter32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Bytes LanToWan WAN side since last restart of service"
::= { bwPortEntry 5 }

bwPortNumber OBJECT-TYPE
SYNTAX Unsigned32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Port Number"
::= { bwPortEntry 6 }

bandwidthPassThrough OBJECT IDENTIFIER
::= { bandwidth 3 }

bwPassThroughIn OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Amount of incoming pass through traffic"
::= { bandwidthPassThrough 1 }

bwPassThroughOut OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Amount of outgoing pass through traffic"
::= { bandwidthPassThrough 2 }

bwPassThroughTotal OBJECT-TYPE
SYNTAX Counter64
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "Total passthrough traffic"
::= { bandwidthPassThrough 3 }

```

```
datastore OBJECT IDENTIFIER
 ::= { statistics 4 }

hitsTotal OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Total number of datastore hits since last restart of
service"
    ::= { datastore 1 }

missTotal OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION
        "Total number of datastore misses since last restart of
service"
    ::= { datastore 2 }

END
```





# Glossary

**ARP.** Address Resolution Protocol. An IP protocol used to obtain a node's physical address.

**Bandwidth.** The upper limit on the amount of data, typically in kilobits per second (kbps), that can pass through a network connection. Greater bandwidth indicates faster data transfer capability.

**Bit.** A Binary digit. The smallest unit of information handled by a computer; either 1 or 0 in the binary number system.

**Blade.** One component in a system that is designed to accept some number of components (blades).

**Bottleneck.** A node in a network at which information is processed more slowly, or any element (for example, a network interface card) that slows network connectivity rates

**CIFS.** Common Internet File System. CIFS is the remote file system access protocol used by Windows servers and clients to share files across the network.

**Database Cursor.** A record pointer in a database. When a database file is selected and the cursor is opened, the cursor points to the first record in the file. Using various commands, the cursor can be moved forward, backward, to top of file, bottom of file and so forth.

**Default gateway.** The default address of a network or Web site. It provides a single domain name and point of entry to the network or site.

**DHCP.** Dynamic Host Configuration Protocol. Software that automatically assigns IP addresses to client stations logging onto a TCP/IP network.

**Domain.** In the Internet, a portion of the Domain Name Service (DNS) that refers to groupings of networks based on the type of organization or geography.

**DNS.** Domain Name Service. System used in the Internet for translating names of network nodes into IP addresses. A Domain Name Server notifies hosts of other host IP addresses, associating host names with IP addresses.

**Ethernet.** The most widely used Local Area Network (LAN) access method.

**FDDI.** Fiber Distributed Data Interface. A set of American National Standards Institute (ANSI) protocols for sending digital data over fiber optic cable. FDDI networks are token-passing networks, and support data rates of up to 100 Mbps (100 million bits) per second. FDDI networks are typically used as backbones for Wide-Area Networks (WANs).

**Filer.** An appliance that attaches to a computer network and is used for data storage.

**Gateway.** A computer that acts as an intermediate device for two or more networks that use the same protocols. The gateway functions as an entry and exit point to the network. Transport protocol conversion might not be required, but some form of processing is typically performed.

**Gigabit Ethernet.** An Ethernet technology that raises transmission speed to 1 Gbps (1000 Mbps).

**Hashing.** Producing hash values for accessing data or for security. A hash value, is a number generated from a string of text. The hash is substantially smaller than the text itself and it is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

**Heartbeat.** A repeating signal transmitted from one appliance to another that indicates that the appliance is operating.

**Heuristic.** A method of problem solving using exploration and trial and error methods. Heuristic program design provides a framework for solving the problem in contrast with a fixed set of rules (algorithmic) that cannot vary.

**Host.** A computer or other computing device that resides on a network.

**Host address.** The IP address assigned to each computer attached to the network.

**Host name.** Name given to a computer, usually by DNS.

**HSRP.** Hot Standby Routing Protocol. HSRP is a routing protocol from Cisco that provides backup to a router in the event of failure. Using HSRP, several routers are connected to the same segment of an Ethernet, FDDI or token-ring network and work together to present the appearance of a single virtual router on the LAN. The routers share the same IP and MAC addresses, therefore in the event of failure of one router, the hosts on the LAN are able to continue forwarding packets to a consistent IP and MAC address. The process of transferring the routing responsibilities from one device to another is transparent to the user.

**HTTP.** Hypertext Transport Protocol. The protocol used by Web browsers to communicate with Web servers.

**HTTPS.** Hypertext Transport Protocol Secure. The protocol for accessing a secure Web server. Using HTTPS directs the message to a secure port number to be managed by a security protocol.

**Interface.** The point at which a connection is made between two elements, systems, or devices so that they can communicate with one another.

**Internet.** The collection of networks tied together to provide a global network that use the TCP/IP suite of protocols.

**IP.** Internet protocol. Network layer protocol in the TCP/IP stack that enables a connectionless internetwork service.

**IP address.** In IP version 4 (IPv4), a 32-bit address assigned to hosts using the IP protocol. Also called an Internet address.

**IPsec.** Internet Protocol Security Protocol. A set of protocols to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. For IPsec to work, the sending and receiving devices must share a public key.

**Latency.** Delay between a request being issued and its response being received.

**Layer-4.** A communications protocol (called the transport layer) responsible for establishing a connection and ensuring that all data has arrived safely. The application delivers its data to the communications system by passing a stream of data Bytes to the transport layer along with the socket (the IP address of the station and a port number) of the destination machine.

**MAPI.** Messaging API. A programming interface from Microsoft that enables a client application to send and receive mail from Exchange Server or a Microsoft Mail (MS Mail) messaging system. Microsoft applications such as Outlook, the Exchange client, and Microsoft Schedule use MAPI.

**Microsoft Exchange.** Messaging and groupware software for Windows from Microsoft. The Exchange server is an Internet-compliant messaging system that runs under Windows systems and can be accessed by Web browsers, the Windows In-box, Exchange client, or Outlook. The Exchange server is also a storage system that can hold anything that needs to be shared.

**Netmask.** A 32-bit mask which shows how an Internet address is divided into network, subnet, and host parts. The netmask has ones in the bit positions in the 32-bit address which are used for the network and subnet parts, and zeros for the host part. The mask must contain at least the standard network portion (as determined by the class of the address), and the subnet field should be contiguous with the network portion.

**Neural Network.** A modeling technique based on the observed behavior of biological neurons and used to mimic the performance of a system. It consists of a set of elements that start out connected in a random pattern, and, based upon operational feedback, are molded into the pattern required to generate the required results. It is used in applications such as robotics, diagnosing, forecasting, image processing and pattern recognition.

**NFS.** Network File System. The file sharing protocol in a UNIX network.

**NIS.** Network Information Services. A naming service that allows resources to be easily added, deleted or relocated.

**OSPF.** Open Shortest Path First. An interior gateway routing protocol developed for IP networks based on the shortest path first or link-state algorithm. Routers use link-

state algorithms to send routing information to all nodes in an internetwork by calculating the shortest path to each node based on a topography of the Internet constructed by each node. Each router sends that portion of the routing table (keeps track of routes to particular network destinations) that describes the state of its own links. It also sends the complete routing structure (topography).

**Packet.** A unit of information transmitted, as a whole, from one device to another on a network.

**Probe.** A small utility program that is used to investigate, or test, the status of a system, network or Web site.

**Policy.** Routing and Quality of Service (QoS) scheme that forwards data packets to network interfaces based on user-configured parameters.

**Port.** A pathway into and out of the computer or a network device such as a hub, switch, or router. On network devices, the ports are for communications, typically connecting Ethernet cables or other network devices.

**Router.** A device that forwards data packets from one LAN or WAN to another. Based on routing tables and routing protocols, routers read the network address in each transmitted frame and make a decision on how to send it based on the most expedient route (traffic load, line costs, speed, bad lines, etc.). Routers work at Layer-3 in the protocol stack, whereas bridges and switches work at the Layer-2.

**SMB.** Server Message Block. A message format used by DOS and Windows to share files, directories and devices. There are also a number of products that use SMB to enable file sharing among different operating system platforms. A product called Samba, for example, enables UNIX and Windows machines to share directories and files.

**SNMP.** Simple Network Management Protocol. A network protocol that provides a way to monitor network devices, performance, and security and to manage configurations and collect statistics.

**Switch.** A network device that filters and forwards frames based on the destination address of each frame. The switch operates at Layer-2 (data link layer) of the Open System Interconnection (OSI) model.

**Tcl.** Tool Command Language. A scripting language for developing cross-platform applications. Tcl is an interpreted language that runs on Windows, UNIX, and Macintosh operating systems. An associated add-on toolkit, Tk (Toolkit) allows you to easily create graphical applications.

**TCP.** Transmission Control Protocol. The error correcting Transport layer (Layer-4) in the TCP/IP protocol suite.

**TCP/IP.** Transmission Control Protocol/Internet Protocol. The protocol suite used in the Internet, intranets, and extranets. TCP provides transport functions, which ensures that the total amount of Bytes sent is received correctly at the other end. TCP/IP is a routable protocol, and the IP part of TCP/IP provides this capability.

# Index

## A

- Administrative password, setting 129
- Admission Control alarm status 185
- Alarm status
  - admission control 185
  - Data Store 185
  - licensing 185
  - link state 185
  - memory paging 186
  - network bypass 186
  - optimization service 186
  - PFS
    - connection error 187
    - operation failed 187
    - partition full 186
  - RAID 187
  - service alarm 186
  - software version mismatch 187
  - System Disk Full 187
  - temperature 187
- Alarm Status report 188
- Alarm status, viewing 185
- Alarm thresholds, setting 116
- Appliance logs, viewing 201
- Asymmetric routing
  - auto-detection
    - about 66
    - enabling 67
  - cache, enabling 67
- Authentication
  - enabling 70
  - setting 127
- Auto-detection of asymmetric routing, about 66
- Auto-discovery rules, overview of 27
- Auxiliary Interface, setting 58

## B

- Backup appliance, setting 73
- Bandwidth Optimization report 148
- Bypass Mode state 16

## C

- CIFS
  - optimization, configuring 31
  - transparent prepopulation
    - enabling 32
    - overview of 47
- Clock synchronization 126
- Configuring, CIFS optimization 31
- Connected Appliances report 166
- Connection forwarding
  - enabling 69
  - setting 68
- Connection history, viewing 167
- Connection limit state 16
- Connection limit, setting 25
- Connection Pooling report, viewing 174
- Connection pooling, enabling 44
- Console
  - connecting to 13
  - navigating 16
- CPU Utilization alarm status 185
- CPU Utilization report 188
- Creating port labels 114
- Critical state 16
- CSV file, exporting statistics to 196
- Current connections
  - viewing 170
  - viewing details 172

## D

- Data Reduction report 152
- Data Store
  - alarm status 185
  - reports 162
- Data store
  - corrupted 16
  - hit rate 150
- Date and time, setting 125
- Degraded state 16
- Deny in-path rules, overview of 27
- Discard in-path rules, overview of 27

- DNS
  - server 62
  - setting 61
- Duplex, tips for setting 54
- E**
- Email notification, setting 117
- Enabling
  - asymmetric routing
    - auto-detection 67
    - cache 67
  - connection forwarding 69
  - encryption 70
  - NetFlow 77
  - NFS optimization 38
  - peering rules 79
  - PFS 99
  - QoS classification 82
  - WCCP groups 94
- Encryption, enabling 70
- Enterprise MIB
  - accessing 209
  - example of 211
- Event and failure notification, setting 117
- Exchange 2003 support, enabling 35
- Exchange port, setting for firewalls 36
- F**
- Failover 73
- Fixed-target rules, overview of 27
- FTP proxies, setting 64
- H**
- Healthy state 16
- Help, table of contents 202
- Host name
  - modifying 63
  - specifying 63
- Hosts, mapping to IP addresses 63
- I**
- In-path
  - interfaces, modifying 54
  - physical, overview of 22
  - rule descriptions 30
  - rules, setting 25
  - static network routes, setting 60
  - support, enabling 23
  - virtual, overview of 22
- Interactive ports
  - forwarding traffic on 113
  - list of 205
- Interface statistics, viewing 177

- Introduction 7
- IP addresses, mapping host to 63

- K**
- Kickoff, reset existing client connections upon startup 24

- L**
- Layer 4 switch support, overview of 24
- Licenses, managing 137
- Licensing alarm status 185
- Link state alarm status 185
- Link State report 178
- Local logging, setting 123

- M**
- MAPI
  - Exchange
    - out-of-path deployments 34
    - ports 34
  - protocol options, setting 34
  - transparent prepopulation, enabling 36
- Memory Paging
  - alarm status 186
  - reports 190
- Message of the day
  - See MOTD
- MIB file
  - accessing 209
  - example of 211
  - SNMP traps sent 210
- Modifying
  - host name 63
  - in-path descriptions 30
  - NFS server settings 39
  - PFS share details 110
  - port labels 115
  - primary interface 52
  - QoS class 85
  - QoS descriptions 89
  - WCCP service group settings 96
- Monitor password, setting 130
- Monitored ports, setting 121
- MOTD, setting 136
- MS-SQL protocol support, enabling 36
- MTU value, setting 54, 57, 59

- N**
- Neighbor Statistics report 181
- NetFlow, enabling 77
- Network Bypass alarm status 186
- NFS
  - optimization, enabling 38
  - server settings 39

- Statistics report 155
  - V2/V4 alarm status 186
  - NSPI port, setting 35
  - NTP servers, setting 125, 126
- O**
- Optimization service alarm status 186
  - Out-of-path, overview of 22
  - Overlapping open 34
  - Overview
    - of asymmetric routing auto-detection 66
    - of CIFS transparent prepopulation 47
    - of fixed-target rules 27
    - of NFS optimization 38
    - of pass-through rules 27
    - of port labels 113
    - of QoS 82
- P**
- Pass-through rules, overview of 27
  - PBR, overview of 24
  - Peering rules, enabling 79
  - PFS
    - connection error alarm status 187
    - enabling 99
    - enabling shares 106
    - initial synchronization 106
    - mapping shares 107
    - modifying share details 110
    - modifying share settings 109
    - operation failed alarm status 187
    - partition full alarm status 186
    - setting shares 103
    - share settings 102
    - upgrading from v2.x to 3.x 107
    - viewing PFS statistics 193
    - viewing status 192
  - Physical in-path, overview of 22
  - Port labels
    - creating 114
    - in-path rules for 25
    - modifying 115
    - overview of 113
  - Ports
    - commonly excluded 204
    - commonly optimized 204
    - default listening 203
    - interactive ports forwarded 205
    - secure automatically forwarded 206
  - Prepopulation
    - enabling shares 47
    - initial synchronization 47
    - modifying share details 49, 51
    - modifying share settings 49
    - overview of 46
  - Primary interface
    - modifying 52
    - setting 52
  - Priorities, QoS 82
- Q**
- QoS**
- class, modifying 85
  - classification, enabling 82
  - overview of 82
  - priorities 82
  - rule descriptions, modifying 89
  - service ports for multiple mappings 90
  - setting rules for 81, 87
  - Statistics report 182
- R**
- RADIUS authentication method, setting 127
  - RAID alarm status 187
  - RBT-Proto, common ports used by the system 203
  - Rebooting 145
  - Remote logging, setting 124
  - Reports
    - Alarm Status 185, 188
    - Bandwidth Optimization 148
    - Connected appliances 166
    - Connection History 167
    - Connection Pooling 174
    - CPU Utilization 188
    - Current Connections 170
    - Current Connections Details 172
    - Data Reduction 152
    - Data Store 162
    - Data Store Hits 150
    - Export Performance Statistics 196
    - Interface Statistics 177
    - Link State 178
    - Memory Paging 190
    - Neighbor Statistics 181
    - NFS Statistics 155
    - PFS Share Status 192
    - PFS Statistics 193
    - QoS Statistics 182
    - System Dumps 197
    - System Snapshots 198
    - TCP Dump 199
    - TCP Statistics 163
    - Throughput 157
    - Traffic Summary 159
  - Resetting existing client connections upon startup 24
  - Restarting, services 144
  - Routing
    - asymmetric, auto-detection of 66
    - enabling simplified 92

## S

- Scheduled jobs, viewing 139
- Secure ports
  - automatically forwarded 206
  - forwarding traffic on 113
- Secure-CIFs feature, enabling 33
- Serial clustering 79
- Service alarm status 186
- Service halted 16
- Service ports, setting 90
- Services, starting, stopping, restarting 144
- Setting
  - alarm thresholds 116
  - auxiliary interface 58
  - backup appliance 73
  - clock synchronization 126
  - date and time 125
  - DNS 61
  - email notification 117
  - event notification 117
  - failure notification 117
  - FTP proxies 64
  - in-path static network routes 60
  - local logging 123
  - Message of the day 136
  - monitored ports 121
  - MOTD 136
  - NTP servers 125, 126
  - PFS shares 103
  - primary interface 52
  - QoS rules 81, 87
  - remote logging 124
  - service groups for WCCP 94
  - SNMP parameters 119
  - SNMP trap receivers 120
  - static network routes 59
  - Web proxies 64
- Setting connection forwarding 68
- Share settings, PFS 102
- Shutting down 145
- Simplified routing, enabling 92
- SMB signing disabling 33
- SNMP
  - MIB, accessing 209
  - parameters, setting 119
  - trap receivers, setting 120
  - traps, summary of sent 210
- Software Version Check alarm status 187
- Software, upgrading 142
- Specifying, host name 63
- Speed and duplex settings 54

- Starting, services 144
- Static main route 60
- Static network routes, setting 59
- Status bar, overview of 16
- Stopping, services 144
- Synchronized data store 73
- System
  - dumps, viewing 197
  - snapshots, viewing 198
- System Disk Full alarm status 187

## T

- TACACS+ authentication method, setting 127
- TCP
  - dump, viewing 199
  - high speed, enabling 42
  - statistics report, viewing 163
- Technical support, contacting 202
- Temperature alarm status 187
- Throughput report 157
- Traffic Summary report 159
- Transparent prepopulation
  - modifying
    - share details 49, 51
  - modifying share settings 49
  - overview
    - of 46
- Traps, summary of SNMP traps sent 210

## U

- Unlicensed state 16
- Upgrading
  - software 142

## V

- Virtual in-path, overview of 22

## W

- WCCP
  - overview of 24
  - service groups
    - settings, modifying 96
  - service groups, enabling 94
  - setting service groups for 94
- Web proxies, setting 64